

7 Verwendung von Behandlungsdaten für interne Qualitätssicherung und Eigenforschung

7.1 Verwendung von Behandlungsdaten in unveränderter Form durch den Behandler



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in unveränderter Form für Zwecke der Forschung oder Qualitätssicherung durch den Behandler genutzt werden?

Aufgrund der unveränderten Form der Behandlungsdaten sind diese noch eindeutig personen- bzw. patientenbezogen, so dass in jedem Fall eine datenschutzrechtliche Erlaubnis für die erfolgende Zweckänderung erforderlich ist.

Bei einer Nutzung der Patientendaten durch den Behandler selbst, gleich zu welchen Zwecken, liegt allerdings kein Offenbaren im Sinne von § 203 StGB vor, da kein Dritter Kenntnis von den der Schweigepflicht unterliegenden Geheimnissen erhält. Aus diesem Grund ist auch für die Nutzung personenbezogener Patientendaten zu Zwecken der Forschung und Qualitätssicherung durch den Behandler selbst keine Entbindung von der Schweigepflicht oder eine gesetzliche Offenbarungsbefugnis notwendig.⁷²⁰

⁷²⁰ Jedenfalls solange die Zugriffsmöglichkeiten für Dritte im Rahmen der Zweckänderung nicht erweitert werden. Es wird im Rahmen dieser Frage davon ausgegangen, dass auf die Forschungsergebnisse, soweit sie noch personenbezogen sind, regulär lediglich der Behandler Zugriff hat (interne IT-Administratoren, der Zugriff kaum auszuschließen ist, gelten insoweit als zulässige Gehilfen ohne besonderen Rechtfertigungsbedarf).

7.1.1 Zweckänderung hin zur Forschung

7.1.1.1 Gesetzliche Erlaubnisse

Gesetzliche Forschungsklauseln, die eine entsprechende Zweckänderung jedenfalls für die interne „Umwidmung“ der Bestimmung der Daten grundsätzlich auch ohne Einwilligung gestatten können, existieren in allen anwendbaren datenschutzrechtlichen Regelungen, d.h. insbesondere auch im Bund (BDSC) und in allen Bundesländern. Zu den Voraussetzungen im Einzelnen sei auf die jeweils zu den Forschungsklauseln gemachten Ausführungen in vorigem Kapitel I.6 verwiesen.⁷²¹

Ob diese Voraussetzungen vorliegen ist auch bei bloßem Datenumgang durch den Behandler in der Regel eine Frage des Einzelfalls, die abhängig vom einzelnen Forschungsvorhaben ist. Allerdings wird im Rahmen der Auslegung und einer gegebenenfalls vorzunehmenden Abwägung begünstigend für die wissenschaftliche Forschung zu berücksichtigen sein, dass es sich vorliegend um Eigenforschung nicht nur der behandelnden Einrichtung, sondern sogar ausschließlich des behandelnden Arztes handelt.

Die auf Krankenhäuser anwendbaren Gesetze mancher Bundesländer enthalten jedoch auch Klauseln, die für bestimmte Formen der rein internen Datenverwendung zu Forschungszwecken weder einen Vorhabensbezug noch eine Interessenbewertung bzw. -abwägung verlangen. In den Grenzen dieser Klauseln ist ein Datenumgang durch den behandelnden Arzt damit ohne Einzelfallabwägung generell zulässig.⁷²² Dabei handelt es sich um folgende Vorschriften:

- Baden-Württemberg: § 15 Abs. 3 LDSC BW
 - Anwendbar auf alle Kliniken des Landes oder diesem zugeordneter Träger (Anstalten, Stiftungen oder Körperschaften wie Kommunen) ohne eigene Rechtspersönlichkeit. Solche Eigen- oder Regiebetriebe sind im Krankenhausbereich aber praktisch kaum mehr anzutreffen.
 - Eine „Speicherung oder Nutzung für andere Zwecke“ liegt nicht vor, „wenn sie [...] Zwecken der Durchführung eigener wissenschaftlicher Forschung der speichernden Stelle dient“.
- Bayern: Art. 27 Abs. 4 S. 1 LKHG BY
 - Anwendbar auf alle Kliniken des Landes oder diesem zugeordneter Träger einschließlich der Universitätskliniken sowie private Plankrankenhäuser und Kliniken der Kirchen.
 - Nutzung (im weiteren Sinne, einschließlich der Speicherung) für Forschungszwecke im Krankenhaus oder im Forschungsinteresse des Krankenhauses ist gestattet; Datenhaltung aber nur intern, externe Forscher können aber im Krankenhaus Zugriff sowie u.U. auch lesenden Fernzugriff erhalten.
- Bremen: § 8 KHDSC HB
 - Anwendbar auf alle Kliniken in Bremen mit Ausnahme derer des Bundes und der Kirchen.

⁷²¹ S. oben S. 87ff.

⁷²² Auch insoweit ist allerdings ausnahmsweise eine Einzelfallabwägung angezeigt, wenn ein betroffener Patient Widerspruch gegen die entsprechende Datenverwendung einlegt.

- Anlage (einschließlich interner Speicherung) medizinischer Dateien durch Angehörige eines Heil- oder Gesundheitsfachberufes für eigene Forschungszwecke ist erlaubt; nicht aber ein Zugriff durch Dritte, soweit dies nicht zur Mitbehandlung erforderlich ist; letztlich darf also nur behandelndes Personal auch zu Forschungszwecken zugreifen (enger als Fachabteilungsgrenze).
- Mecklenburg-Vorpommern: § 38 Abs. 6 LKHG MV
 - Anwendbar auf alle Kliniken in Mecklenburg-Vorpommern mit Ausnahme solcher des Bundes.
 - Anlage (einschließlich interner Speicherung) von Dateien durch Ärzte für eigene Forschungszwecke ist gestattet, nicht jedoch ein Zugriff durch Dritte, soweit dies nicht zur Mitbehandlung erforderlich ist; letztlich darf also nur behandelndes Personal auch zu Forschungszwecken zugreifen (enger als Fachabteilungsgrenze).
- Nordrhein-Westfalen: § 6 Abs. 2 S. 1 GDStG NW
 - Anwendbar auf alle Kliniken des Landes oder diesem zugeordneter Träger sowie private Plankrankenhäuser.
 - Wissenschaftliches Personal darf zu Zwecken der wissenschaftlichen Forschung Patientendaten nutzen (im engeren Sinne, d.h. intern und ohne separate Speicherung), auf die es in den Einrichtungen aufgrund seiner Behandlungstätigkeiten ohnehin Zugriff hat (also nur für behandelndes Personal, enger als Fachabteilungsgrenze).
- Thüringen: § 27 Abs. 4 S. 1 LKHG TH
 - Anwendbar auf alle Kliniken in Thüringen mit Ausnahme solcher des Bundes.
 - Nutzung (im weiteren Sinne, einschließlich der Speicherung) für Forschungszwecke im Krankenhaus oder im Forschungsinteresse des Krankenhauses ist gestattet; Datenhaltung aber nur intern, externe Forscher können aber im Krankenhaus Zugriff sowie u.U. auch lesenden Fernzugriff erhalten (praktisch identisch mit Art. 27 Abs. 4 S. 1 LKHG BY).

7.1.1.2 Einwilligung als Alternative

Soweit keine gesetzliche Erlaubnis für die zweckändernde Datenverwendung vorliegt, kommt im Rahmen der jeweiligen Vorschriften und deren überwiegend gleichwertigen Voraussetzungen (Informiertheit, Bestimmtheit, Freiwilligkeit usw.) eine Einwilligung als Rechtsgrundlage in Betracht.⁷²³

Manche Bundesländer fordern in ihren auf Kliniken anwendbaren Gesetzen allerdings, dass die Einwilligung „im Einzelfall“ erteilt wird. Die sind

- Baden-Württemberg (§ 50 Abs. 1 Hs. 1 LKHG BW),
- Bremen (§ 2 Abs. 1 KHDSG HB),
- Mecklenburg-Vorpommern (§ 33 Abs. 1 LKHG MV) und das
- Saarland (§ 13 Abs. 2 S. 2 LKHG SL).

Insofern sollte man insbesondere nicht schon bei Aufnahme in die Klinik eine „prophylaktische“ Einwilligung verlangen, sondern erst, wenn die bei der Behandlung

⁷²³ Zu den allgemeinen Voraussetzungen wie sie exemplarisch zum BDSG näher beschrieben wurden s. oben S. 110ff.

angefallenen Daten auch für den Patienten überschaubar sind und der Forschungswunsch des behandelnden Arztes sich zumindest etwas konkretisiert hat.

Einige Bundesländer gestatten in ihren auf Kliniken anwendbaren Gesetzen zudem auch die Einwilligung im Forschungsbereich nur für bestimmte Vorhaben. Dies sind

- Berlin (§ 25 Abs. 1 S. 1 LKHG BE: krankenhausinterne Forschungsvorhaben),⁷²⁴
- Bremen (§ 7 Abs. 1 KHDG HB: wissenschaftliche medizinische Forschungsvorhaben, gilt aber nicht für interne Dateien nach § 8 KHDG HB),⁷²⁵
- Hamburg (§ 12 Abs. 2 Nr. 2 LKHG HH: bestimmtes Forschungsvorhaben; wird aber durch § 12a LKHG HH ergänzt, der Übernahme in Sammlungen zu allgemeinen Forschungszwecken gestattet),⁷²⁶
- Rheinland-Pfalz (§ 37 Abs. 1 S. 1 Hs. 1 LKHG RP: interne Forschungsvorhaben)⁷²⁷ sowie das
- Saarland (§ 14 Abs. 2 S. 1 LKHG SL: bestimmte Forschungsvorhaben).⁷²⁸

Insofern wird man auch dem behandelnden Arzt selbst mit Einwilligung des Patienten keine Anlage eines allgemeinen personenbezogenen Forschungsregisters unabhängig von konkreten Vorhaben erlauben können, sei es auch nur für eigene Zwecke.

In Bremen schränkt der aufgelistete, vorhabenbezogene § 7 Abs. 1 KHDG HB letztlich aber die Eigenforschung des behandelnden Arztes nicht entsprechend ein, denn dort sind schon auf rein gesetzlicher Basis über § 8 KHDG HB eigene Forschungsdateien erlaubt.

In Bezug auf Hamburg schadet der für die Einwilligung in § 12 Abs. 2 Nr. 2 LKHG HH geforderte Vorhabensbezug insoweit nicht, als dass mit § 12a LKHG HH eine Sonderregelung für die Übernahme von Patientendaten in Sammlungen zu allgemeinen Forschungszwecken mit Einwilligung des Patienten geschaffen wurde, auf welche sich auch der behandelnde Arzt berufen kann.

7.1.1.3 Pseudonymisierungs- und Anonymisierungspflichten

Allerdings wird in den gesetzlichen Forschungsklauseln eine Pseudonymisierung und Anonymisierung der Daten gefordert, zumindest sobald dies ohne Gefährdung des Forschungszweckes möglich ist. Daraus folgt, dass die unveränderte Verwendung von Behandlungsdaten zu Forschungszwecken in aller Regel jedenfalls kein Dauerzustand, sondern nur ein Durchgangsstadium sein darf. Soweit der Forschungszweck jedoch zwingend (noch) den unveränderten Umgang erfordert, ist dies allerdings, wenn die übrigen Voraussetzungen der Forschungsklauseln vorliegen, nicht ausgeschlossen, so zum Beispiel zur Pseudonymgenerierung. Eine Übersicht zu den entsprechenden Regelungen findet sich im folgenden Abschnitt.⁷²⁹

Im Anwendungsbereich des BDSG, also für Arztpraxen und Kliniken des Bundes oder auch anderer Träger, soweit § 40 Abs. 2 S. 2 BDSG auf diese subsidiär anwendbar ist,

724 Näheres s.o. S. 149f.

725 Näheres s.o. S. 160f.

726 Näheres s.o. S. 167.

727 Näheres s.o. S. 194f.

728 Näheres s.o. S. 204f.

729 S. unten S. 244f.

ist allerdings eine sofortige Pseudonymisierung bei Zweckänderung hin zur Forschung nötig. Entsprechende Anordnungen treffen auch das KHEG Brandenburg und das LKHG Sachsen-Anhalt. Gleiches gilt für das LDSG Baden-Württemberg, welches insoweit auch auf manche dem LKHG BW unterworfenen Kliniken subsidiär anwendbar ist, da dieses LKHG keine Regelungen zur Pseudonymisierung und Anonymisierung im Forschungskontext unabhängig von einer Datenübermittlung enthält. In den entsprechenden Einrichtungen ist daher ein unveränderter Umgang mit Behandlungsdaten zu Forschungszwecken jedenfalls allein auf gesetzlicher Grundlage grundsätzlich unzulässig.

Ausgenommen von diesem Grundsatz sind aber die (sofortige) Pseudonymgenerierung, die Aufrechterhaltung der Pseudonym-Patienten-Zuordnung (durch abgeschottete Speicherung) sowie die Re-Identifikation, wenn dies aus besonderen Gründen nötig werden sollte und die Voraussetzungen entsprechender Zulässigkeitstatbestände vorliegen, denn die Pseudonymisierung soll im Gegensatz zur Anonymisierung gerade eine Identifizierung in begründeten Fällen ermöglichen.⁷³⁰ So könnte zum Beispiel eine Re-Identifizierung erfolgen, wenn die Voraussetzungen einer einschlägigen Forschungsklausel vorliegen und dies zur Rekrutierung geeigneter Probanden für Folgestudien erforderlich ist.⁷³¹ Auch ist an eine Re-Identifizierung zu denken, wenn ein Forschungsergebnis für die fortdauernde Behandlung innerhalb der Einrichtung relevant werden sollte.⁷³² Das LKHG Hamburg regelt als einziges LKHG explizit die Aufnahme von Daten in ein allgemeines Forschungsregister, verlangt hiervor jedoch, selbst wenn – wie dort vorgeschrieben – eine Einwilligung vorliegt, zumindest die Pseudonymisierung der Daten (§ 12a Abs. 2 LKHG HH). Dieses Erfordernis lässt sich jedenfalls für Kliniken im Anwendungsbereich des LKHG HH somit auch nicht mit Einwilligung der Patienten durchbrechen.

Im Übrigen, also soweit eine Pseudonymisierung oder Anonymisierung nicht explizit auch für den Fall der Einwilligung vorgeschrieben ist, kann jedoch, soweit die jeweiligen Voraussetzungen (Informiertheit, Bestimmtheit, Freiwilligkeit usw.) vorliegen, grundsätzlich mittels einer Einwilligung auch ein Dispens von allgemeinen Pseudonymisierungs- und Anonymisierungspflichten erlangt werden. Dies gilt zumindest bei formularmäßigen Einwilligungen jedoch aufgrund der im Ansatz bundeseinheitlichen AGB-rechtlichen Angemessenheitskontrolle nach § 307 BGB nur mit gewissen Einschränkungen. Denn im Ergebnis ist die Gesetzeslage im Bund und allen Länder insoweit weitgehend einheitlich, als dass jedenfalls eine Pseudonymisierung und Anonymisierung zu erfolgen hat, sobald dies ohne Gefährdung des Forschungszwecks

730 Eine Ausnahme vom zuletzt genannten Punkt dürfte die Pseudonymisierung nach § 15 Abs. 3 TMG sein, der pseudonyme Nutzungsprofile bei Telemedien gestattet, die aber „nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden“ dürfen (S. 3). Die Verwendung des Rechtsbegriffs Pseudonymisierung dient dort also nicht der Erhaltung einer Re-Identifizierungsmöglichkeit, sondern lediglich der Abschwächung der rechtlichen Anforderungen an die technische Umsetzung im Vergleich zur (auch nur faktischen) Anonymisierung. Im vorliegenden Kontext der Sekundärnutzung med. Behandlungsdaten dürfte § 15 Abs. 3 TMG jedoch keine Rolle spielen, denn selbst bei telemedizinischen Anwendungen gelten für die über das Telemedium transportierten personen- und gesundheitsbezogenen Inhalte die allgemein für Gesundheitsdaten maßgeblichen Vorschriften.

731 S. oben den entspr. Exkurs in Kap. I.4.1.2.5, S. 45ff.

732 Insoweit dürfte auch die Bindung an den Zweckrahmen der wissenschaftlichen Forschung, wie sie u.a. in § 40 BDSG enthalten ist, nicht entgegenstehen. Diese würde dann zwar für Behandlungszwecke durchbrochen, was aber auf Grundlage der jeweiligen den Datenumgang zu Behandlungszwecken erlaubenden Normen (ausnahmsweise) zulässig sein dürfte. Hilfsweise käme die (mutmaßliche) Einwilligung oder Ausnahmenormen wie § 28 Abs. 6 Nr. 1 BDSG (Schutz lebenswichtiger Interessen des Betroffenen) in Betracht.

und ohne unverhältnismäßigen Aufwand möglich ist.⁷³³ Deshalb wird man davon ausgehen müssen, dass jedenfalls ein Mindestmaß an Pseudonymisierung auch mittels einer Einwilligung selbst bei Datenverwendung zu Forschungszwecken nur durch den Behandler in der Regel nicht dauerhaft vollkommen umgangen werden kann. Gerade für diejenigen Länder, deren Gesetze eine sofortige Pseudonymisierung vorsehen, eröffnet die Einwilligung jedoch einen erweiterten Spielraum.

7.1.1.4 Übersicht 3: Spezifische Pflichten zur Pseudonymisierung oder Anonymisierung für die Forschung unabhängig von einer Datenübermittlung

Aus der folgenden Übersicht (s. Tab. 5) lassen sich die Rechtsgrundlagen für eine Anonymisierung oder Pseudonymisierung beim Datenumgang zu Forschungszwecken im Anwendungsbereich der jeweils genannten Gesetze entnehmen. Dabei werden nicht nur die vorrangig geltenden (Landeskrankenhaus-)Gesetze berücksichtigt, sondern auch die jeweils nachrangig heranziehbaren Gesetze, die eingreifen, soweit das vorrangige Gesetz keine Regelung enthält.

Tab. 5 Übersicht 3: Spezifische Pflichten zur Pseudonymisierung oder Anonymisierung für die Forschung unabhängig von einer Datenübermittlung

Form der Reduktion des Personen- bezugs Anwendungs- bereich des	Pseudonymisierung	Anonymisierung
BDSG	§ 40 Abs. 2 S. 2 BDSG: sofort	§ 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
LKHG Baden-Württemberg	§ 35 Abs. 2 S. 2 LDSG BW, § 40 Abs. 2 S. 2 BDSG: sofort	§ 35 Abs. 2 S. 1 LDSG BW, § 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
LKHG Bayern	§ 40 Abs. 2 S. 2 BDSG: sofort	§ 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
LKHG Berlin	§ 25 Abs. 2 S. 1 LKHG BE: sofort, soweit angemessen (i.E. sobald wie möglich)	§ 25 Abs. 2 S. 1 LKHG BE: sobald wie nach dem Forschungszweck möglich
KHEG Brandenburg	§ 28 Abs. 2 S. 2 LDSG BB: sofort	§ 28 Abs. 2 S. 1 LDSG BB: sobald wie nach dem Forschungszweck möglich
KHDSG Bremen	§ 7 Abs. 4 S. 1 KHDSG HB: sobald wie nach dem Forschungszweck möglich	§ 7 Abs. 4 S. 2, § 8 S. 3 KHDSG HB: sobald wie möglich
LKHG Hamburg	§ 12 Abs. 3 S. 1 LKHG HH: sobald wie nach dem Forschungszweck möglich; § 12a Abs. 2 LKHG HH: in jedem Fall (sofort) vor Aufnahme in Sammlung von Daten zu allg. Forschungszwecken	§ 12 Abs. 3 S. 3 LKHG HH: sobald wie nach dem Forschungszweck möglich; § 12a Abs. 1 S. 3 LKHG HH: kein Einwilligungserfordernis, wenn Daten vor Weitergabe an Sammlung zu allg. Forschungszwecken anonymisiert

⁷³³ Dieser kleinste gemeinsame Nenner der jeweils einschlägigen Gesetze dürfte auch der wesentliche Grundgedanke der jeweiligen gesetzlichen Regelungen sein, weshalb ein Abweichen hiervon nach § 307 Abs. 2 Nr. 1 BGB für den Patienten unangemessen benachteiligend und damit unwirksam wäre.

Anwendungsbereich des	Form der Reduktion des Personenbezugs	
	Pseudonymisierung	Anonymisierung
LKHG Hessen	§ 33 Abs. 2 Hs. 1 LDSG HE: sobald wie nach dem Forschungszweck möglich ; gilt gem. § 12 Abs. 3 LKHG HE auch zwischen Fachabteilungen einer Klinik	§ 33 Abs. 2 Hs. 2 LDSG HE: sobald wie nach dem Forschungszweck möglich ; gilt gem. § 12 Abs. 3 LKHG HE auch zwischen Fachabteilungen einer Klinik
LKHG Mecklenburg-Vorpommern	§ 38 Abs. 4 S. 1 LKHG MV: sobald wie nach dem Forschungszweck möglich	§ 38 Abs. 4 S. 2 LKHG MV: sobald wie nach dem Forschungszweck möglich
LDSG Niedersachsen	§ 40 Abs. 2 S. 2 BDSG: sofort	§ 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
GDSG Nordrhein-Westfalen	§ 6 Abs. 4 GDSG NW: sobald wie nach dem Forschungszweck möglich	§ 6 Abs. 4 GDSG NW: sobald wie nach dem Forschungszweck möglich
LKHG Rheinland-Pfalz	§ 37 Abs. 4 LKHG RP: sobald wie nach dem Forschungszweck möglich	§ 37 Abs. 1 Nr. 3 LKHG RP: kein Einwilligungserfordernis, wenn die Daten vor ihrer weiteren Verarbeitung anonymisiert wurden; § 37 Abs. 4 LKHG RP: sobald wie nach dem Forschungszweck möglich
LKHG Saarland	§ 14 Abs. 8 S. 2 LKHG SL: sobald wie nach dem Forschungszweck möglich	§ 14 Abs. 8 LKHG SL: sobald wie nach dem Forschungszweck möglich
LKHG Sachsen	§ 34 Abs. 4 S. 2 LKHG SN: sobald wie nach dem Forschungszweck möglich	§ 34 Abs. 4 S. 1 LKHG SN: sobald wie nach dem Forschungszweck möglich
LDSG Sachsen-Anhalt	§ 40 Abs. 2 S. 2 BDSG: sofort	§ 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
LDSG Schleswig-Holstein	§ 40 Abs. 2 S. 2 BDSG: sofort	§ 40 Abs. 2 S. 1 BDSG: sobald wie nach dem Forschungszweck möglich
LKHG Thüringen	§ 27a Abs. 4 S. 1 LKHG TH: sobald wie nach dem Forschungszweck möglich	§ 27a Abs. 2 S. 2 LKHG TH: sobald wie nach dem Forschungszweck möglich
PatDSO/ KDO (katholische Kliniken, soweit Öffnungsklausel)	§ 7 Abs. 3 S. 2 PatDSO: sobald wie nach dem Forschungszweck möglich	§ 7 Abs. 3 PatDSO: sobald wie nach dem Forschungszweck möglich
DSG-EKD (evangelische Kliniken, soweit Öffnungsklausel)	§ 25 Abs. 3 S. 2 DSG-EKD: sobald wie nach dem Forschungszweck möglich	§ 25 Abs. 3 S. 1 DSG-EKD: sobald wie nach dem Forschungszweck möglich

7.1.2 Zweckänderung hin zur Qualitätssicherung

7.1.2.1 Gesetzliche Erlaubnisse, Einwilligung als Alternative

Im BDSG findet sich, von der Untersuchung konkreter medizinischer Serienschäden abgesehen (falls man diese überhaupt unter den Begriff der Qualitätssicherung fassen möchte), keine gesetzliche Erlaubnis für die generalisierende Qualitätssicherung, nicht einmal für den entsprechenden internen Datenumgang.⁷³⁴ Das BDSG gilt dabei nicht nur für Arztpraxen und die (wenigen) Kliniken des Bundes, sondern über Verweisungen letztlich auch für alle Kliniken⁷³⁵ in Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein.

Nach den anderen anwendbaren Rechtsgrundlagen ist die Qualitätssicherung, jedenfalls die interne, aufgrund von entsprechenden Erlaubnisnormen grundsätzlich zulässig. Zu den gesetzlichen Voraussetzungen im Einzelnen sei auf die jeweiligen Teile zur Qualitätssicherung in der Darstellung der Rechtsgrundlagen in den einzelnen Bundesländern verwiesen.⁷³⁶ Teils wird hier ebenfalls eine Interessenabwägung gefordert, wenn auch seltener als bei den Forschungsklauseln.

Voraussetzung für einen unveränderten Umgang mit patientenbezogenen Daten zu diesem Zweck ist aber jedenfalls, dass dieser erforderlich ist, der Zweck also nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann. Letzteres wird in manchen Rechtsgrundlagen (über den allgemeinen Grundsatz der Datensparsamkeit und -vermeidung hinaus) noch einmal besonders hervorgehoben. Da es bei der hier betrachteten (generalisierenden) Qualitätssicherung um die Gewinnung genereller Aussagen zum Qualitätsniveau geht, erfordert die unverändert personenbezogene Verwendung eine besondere Rechtfertigung.

Auf der Ebene des Behandlers kann aber aufgrund einer eventuell gewünschten Rücküberführung allgemeiner Qualitätsaussagen in die individuelle Behandlung noch ein rechtfertigender Grund bestehen, möglicherweise auch noch auf Ebene der behandelnden Fachabteilung, aber kaum mehr darüber hinaus. Soweit dieser Bereich verlassen wird, ist – unabhängig davon, ob man insoweit wie manche LKHG eine Gleichstellung mit der Übermittlung annimmt – in aller Regel zumindest eine Pseudonymisierung angezeigt. Auch innerhalb der Fachabteilung wird aus der durch das „soweit“ ersichtlichen sachlichen Einschränkung jedoch mit der Zeit ähnlich wie bei der Forschung ein „sobald“, also letztlich doch eine Anonymisierung oder Pseudonymisierung notwendig werden, spätestens nachdem die Behandlung abgeschlossen wurde.

7.1.2.2 Übersicht 4: Spezifische Pflichten zur Pseudonymisierung oder Anonymisierung für die Qualitätssicherung unabhängig von einer Datenübermittlung

Aus der folgenden Übersicht (s. Tab. 6) lassen sich die Rechtsgrundlagen für eine Anonymisierung oder Pseudonymisierung beim Datenumgang zu Zwecken der Qualitätssicherung im Anwendungsbereich der jeweils genannten Gesetze entnehmen.

⁷³⁴ S. oben S. 108f.

⁷³⁵ Teils von kirchlichen Kliniken abgesehen.

⁷³⁶ S. oben S. 123ff.

Dabei werden nicht nur die vorrangig geltenden (Landeskrankenhaus-)Gesetze berücksichtigt, sondern auch die jeweils nachrangig heranziehbaren Gesetze, die eingreifen, soweit das vorrangige Gesetz keine Regelung enthält.

Tab. 6 Übersicht 4: Spezifische Pflichten zur Pseudonymisierung oder Anonymisierung für die Qualitätssicherung unabhängig von einer Datenübermittlung

Form der Reduktion des Personen- bezugs	Anwendungsbereich des	
	Pseudonymisierung	Anonymisierung
BDSG	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LKHG Baden-Württemberg	§ 9 Abs. 1 LDSG BW: Datensparsamkeit bei der automatisierten Verarbeitung; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 45 Abs. 3 Nr. 1 LKHG BW: soweit nicht anonymisiert erreichbar ; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LKHG Bayern	LKHG: keine Regelungen; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	LKHG: keine Regelungen; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LKHG Berlin	§ 24 Abs. 4 S. 1 Nr. 3 LKHG BE: soweit nicht pseudonymisiert erreichbar	§ 24 Abs. 4 S. 1 Nr. 3 LKHG BE: soweit nicht anonymisiert erreichbar
KHEG Brandenburg	§ 7 Abs. 1 S. 2 LDSG BB: Grundsatz der Datensparsamkeit	§ 28 Abs. 2 S. 1 Nr. 1 KHEG BB: soweit nicht anonymisiert erreichbar ; § 7 Abs. 1 S. 2 LDSG BB: Grundsatz der Datensparsamkeit
KHDSG Bremen	§ 2 Abs. 5 Nr. 1 KHDSG HB: soweit nicht pseudonymisiert erreichbar	§ 2 Abs. 5 Nr. 1 KHDSG HB: soweit nicht anonymisiert erreichbar ; Abs. 6: anonymisieren, sobald der Verarbeitungszweck dies erlaubt
LKHG Hamburg	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LKHG Hessen	§ 12 Abs. 2 Nr. 7 LKHG HE: soweit nicht pseudonymisiert erreichbar	§ 12 Abs. 2 Nr. 7 LKHG HE: soweit nicht anonymisiert erreichbar
LKHG Mecklenburg- Vorpommern	§ 34 Abs. 1 S. 1 Nr. 2 LKHG MV: soweit nicht pseudonymisiert erreichbar ; § 5 Abs. 1 S. 2 LDSG MV: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 34 Abs. 1 S. 1 Nr. 2 LKHG MV: soweit nicht anonymisiert erreichbar ; § 5 Abs. 1 S. 2 LDSG MV: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand

Anwendungsbereich des	Form der Reduktion des Personenbezugs	
	Pseudonymisierung	Anonymisierung
LDSG Niedersachsen	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
GDSG Nordrhein-Westfalen	§ 4 Abs. 2 S. 1 LDSG NW: Datenvermeidung bei informations-technischen Produkten und Verfahren	§ 11 Abs. 2 GDSG NW: soweit nicht anonymisiert erreichbar ; § 4 Abs. 2 S. 1 LDSG NW: Datenvermeidung bei informations-technischen Produkten und Verfahren
LKHG Rheinland-Pfalz	§ 36 Abs. 2 S. 1 Nr. 2 LKHG RP: soweit nicht pseudonymisiert auf vertretbare Weise erreichbar	§ 36 Abs. 2 S. 1 Nr. 2 LKHG RP: soweit nicht anonymisiert auf vertretbare Weise erreichbar
LKHG Saarland	§ 13 Abs. 4 S. 1 Nr. 10 LKHG SL: soweit nicht pseudonymisiert erreichbar	§ 13 Abs. 4 S. 1 Nr. 10 LKHG SL: soweit nicht anonymisiert erreichbar
LKHG Sachsen	§ 9 Abs. 1 S. 2 LDSG SN: Beachtung der Grundsätze zur Datenvermeidung und zur Datensparsamkeit ; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 9 Abs. 1 S. 2 LDSG SN: Beachtung der Grundsätze zur Datenvermeidung und zur Datensparsamkeit ; § 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LDSG Sachsen-Anhalt	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LDSG Schleswig-Holstein	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
LKHG Thüringen	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3a S. 2 BDSG: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
PatDSO/ KDO (katholische Kliniken, soweit Öffnungsklausel)	§ 2a S. 2 KDO: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 3 Abs. 3 PatDSO: soweit nicht anonymisiert erreichbar ; § 2a S. 2 KDO: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand
DSG-EKD (evangelische Kliniken, soweit Öffnungsklausel)	§ 2a S. 2 DSG-EKD: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand	§ 2a S. 2 DSG-EKD: sobald nach dem Verwendungszweck möglich und kein unverhältnismäßiger Aufwand

7.2 Verwendung von Behandlungsdaten in pseudonymisierter Form durch den Behandler



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in pseudonymisierter Form für Zwecke der Forschung oder Qualitätssicherung durch den Behandler genutzt werden? Zu beachten ist hierbei auch der Vorgang der Pseudonymisierung.

7.2.1 Verwendung pseudonymer Daten durch den Behandler

Vorliegend wird davon ausgegangen, dass die Pseudonymisierung durch den Behandler selbst erfolgt, denn andernfalls hätten doch wieder andere Personen Zugriff auf Behandlungsdaten, was durch die Fragestellung ausgeschlossen wird. Der Behandler wird dann aber auch über die ihm bekannte Zuordnungsvorschrift wieder den Personenbezug der pseudonymisierten Daten herstellen können, so dass diese für ihn als personenbezogen gelten.⁷³⁷ Vor diesem Hintergrund stellt die Pseudonymisierung in diesem Szenario „lediglich“ eine Sicherheitsmaßnahme insbesondere für den Fall dar, dass Dritte sich unberechtigterweise Zugriff auf den Datenbestand des forschenden Behandlers oder einen Teil davon (möglicherweise eben nicht die Zuordnungsliste bzw. -vorschrift) verschaffen, um es diesen dann zu erschweren, den Personenbezug herzustellen.⁷³⁸ Daneben wird auch die Wahrnehmung des forschenden Behandlers so eingeschränkt, dass dieser seine Forschungsergebnisse, jedenfalls bei einer größeren Zahl an Datensätzen, i.d.R. nicht mehr unmittelbar intuitiv, sondern nur noch bei Bedarf und durch aktive Zuordnung auf einen Patienten beziehen kann.

Da für den forschenden Behandler damit letztlich ein Personenbezug erhalten bleibt, besteht auch für ihn auch beim Umgang mit den pseudonymisierten Daten ein Verbot mit Erlaubnisvorbehalt. Im Hinblick auf die in Betracht kommenden gesetzlichen Erlaubnisse oder die Einwilligung kann insoweit auf die Antwort zur vorigen Frage verwiesen werden.⁷³⁹

Für die Forschung wird eine Pseudonymisierung, wie bereits ausgeführt, in allen anwendbaren Rechtsgrundlagen früher oder später vorgeschrieben. Selbst durch formelmäßige Einwilligung wird man sie nicht vollkommen umgehen können.

Teilweise finden sich entsprechende Vorgaben, meist in moderaterer Form, explizit auch für die Qualitätssicherung. Im Übrigen greifen die allgemeinen Grundsätze der Erforderlichkeit sowie der Datenvermeidung und -sparsamkeit. Damit spielt die Pseudonymisierung für die Qualitätssicherung eine etwas geringere Rolle als für die Forschung, erleichtert aber auch bei qualitätssichernder Zweckbestimmung die rechtmäßige Datenverwendung.

⁷³⁷ Vgl. Gola/Schomerus, BDSG, § 3 Rdnr. 46.

⁷³⁸ So ordnet beispielsweise § 9 Abs. 1 LDSG BW (wie auch einige andere LDSG) die Grundsätze der Datensparsamkeit und -vermeidung, wie sie durch Pseudonymisierung und Anonymisierung umgesetzt werden können, in den Rahmen der technischen und organisatorischen Sicherheitsmaßnahmen ein.

⁷³⁹ S. oben S. 239ff.

Insgesamt wird man damit auch bei zweckändernder Verwendung lediglich durch den Behandler aufgrund der Pseudonymisierung leichter eine Rechtfertigung, sei es aufgrund von Erlaubnisnormen oder Einwilligungen, annehmen können als bei Verwendung unveränderter Behandlungsdaten.

Beim Pseudonymisieren werden die direkten Identifikationsmerkmale wie der Name durch ein Kennzeichen, das Pseudonym, mit dem Zweck ersetzt, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (vgl. § 3 Abs. 6a BDSG). Letztlich bleibt, wie bereits ausgeführt, für denjenigen, der über die Ersetzungs- bzw. Zuordnungsvorschrift verfügt, jedoch der Personenbezug trotz Pseudonymisierung erhalten.

7.2.2 Vorgang der Pseudonymisierung

Abschließend soll geprüft werden, ob der Vorgang der Pseudonymisierung für sich genommen unter einem datenschutzrechtlichen Erlaubnisvorbehalt steht. Man könnte in der Ersetzung der unmittelbaren Identifikatoren durch ein Pseudonym zunächst ein Verändern personenbezogener Daten sehen, welches einen Unterfall der grundsätzlich rechtfertigungsbedürftigen Datenverarbeitung darstellt. Allerdings setzt ein Verändern im Rechtssinne „das inhaltliche Umgestalten gespeicherter personenbezogener Daten“ voraus (§ 3 Abs. 4 S. 2 Nr. 2 BDSG),⁷⁴⁰ welches beim Pseudonymisieren in der Regel nicht vorliegt, da es hierbei nur um eine Reduktion, nicht aber eine Substitution vorhandener Informationen geht.⁷⁴¹ Zwar werden die Identifikatoren in syntaktischer Hinsicht durch das Pseudonym ersetzt. Dadurch wird aber der Aussagegehalt der Daten nicht in semantischer (inhaltlicher) Hinsicht geändert, sondern lediglich – im Hinblick auf den Personenbezug – verringert.

Aufgrund des mit dem Ersetzen verbundenen Löschsens der Identifizierungsmerkmale (im pseudonymisierten Datensatz) könnte aber doch eine Datenverarbeitung im Rechtssinne (§ 3 Abs. 4 S. 2 Nr. 5 BDSG) und damit ein im Ansatz rechtfertigungsbedürftiger Vorgang vorliegen (§ 4 Abs. 1 BDSG). Andernfalls dürfte der auch eine Erlaubnis erfordernde Auffangtatbestand des Nutzens vorliegen (§ 3 Abs. 5 BDSG). Diese Verwendungsakte (sei es Löschen oder jedenfalls sonstige Formen der Verarbeitung oder hilfsweise das Nutzen) dürften hier auch noch als Verwendung personenbezogener Daten angesehen werden können, da die Pseudonymisierung den Personenbezug gerade für die pseudonymisierende Stelle nicht ausschließt, denn andernfalls läge schon generell eine Anonymisierung vor.⁷⁴²

Somit liegt ein eigenständiger Verwendungsakt vor, der rechtfertigungsbedürftig ist. Allerdings dient dieser Akt der Reduktion des Personenbezugs, weshalb sich kein zusätzlicher Rechtfertigungsbedarf gegenüber der nachfolgenden Verwendung pseudonymer Daten ergibt, jedenfalls wenn diese Daten wie vorliegend für den Verwender noch personenbezogen sind.⁷⁴³ Dies gilt zumal bei gesetzlich vorgeschriebener oder über den Grundsatz der Datensparsamkeit geforderter Pseudonymisierung.

⁷⁴⁰ Bezüglich dieser Begriffsdefinition gibt es keine inhaltlichen Abweichungen nach der Rechtslage in den einzelnen Bundesländern.

⁷⁴¹ Gola/Schomerus, BDSG, § 3 Rdnr. 31. Vergleichbar (bzw. noch eindeutiger) ist die Rechtslage beim Anonymisieren, s. schon oben S. 36 und sogleich S. 251.

⁷⁴² Vgl. oben S. 37f.

⁷⁴³ Zu diesem Ergebnis würde man letztlich auch gelangen, wenn man den Vorgang des Pseudonymisierens für sich genommen keinem Erlaubnisvorbehalt unterstellt, denn schon die nachgelagerte Speicherung (oder sogar nur die temporäre Nutzung) der pseudonymisierten Daten stellt für den Inhaber der Pseudonym-Identität-Zuordnung einen erlaubnispflichtigen Vorgang dar.

7.3 Verwendung von Behandlungsdaten in anonymisierter Form durch den Behandler



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in anonymisierter Form für Zwecke der Forschung oder Qualitätssicherung durch den Behandler genutzt werden? Zu beachten ist hierbei auch der Vorgang der Anonymisierung.

7.3.1 Verwendung anonymen Daten durch den Behandler

Die Verwendung anonymisierter Daten unterliegt keinen datenschutzrechtlichen Restriktionen, d.h. hierfür ist weder eine gesetzliche Erlaubnis noch eine Einwilligung des Betroffenen nötig.⁷⁴⁴ Maßgebend ist lediglich, dass die betrachtete Person oder Stelle keinen Personenbezug (mehr) herstellen kann.⁷⁴⁵ Dies trifft nach der vorliegenden Fragestellung auch auf den Behandler selbst zu.

7.3.2 Vorgang der Anonymisierung

7.3.2.1 Kein Erlaubnisvorbehalt

Letztlich existiert auch kein Erlaubnisvorbehalt für den Vorgang der Anonymisierung.⁷⁴⁶

Dieser setzt zwar an noch personenbezogenen Daten an und verändert diese in gewisser Weise im technischen Sinn, indem zumindest die unmittelbaren Identifikationsmerkmale der betroffenen Personen gelöscht werden.⁷⁴⁷ Wohl aus diesem Grund spricht die Legaldefinition des Anonymisierens in § 3 Abs. 6 BDSG auch von einem „Verändern personenbezogener Daten“.

Jedoch setzt ein Verändern als Unterfall der Datenverarbeitung im Rechtssinne „das inhaltliche Umgestalten gespeicherter personenbezogener Daten“ voraus (§ 3 Abs. 4 S. 2 Nr. 2 BDSG), welches beim Anonymisieren in der Regel nicht vorliegt, da es hierbei nur um eine Reduktion, nicht aber eine Substitution vorhandener Informationen geht.⁷⁴⁸ Somit scheidet ein Verändern im Rechtssinne als Anknüpfungspunkt für einen Erlaubnisvorbehalt aus. Allerdings dürfte auf Grund des Löschsens der Identifizierungsmerkmale dennoch eine Datenverarbeitung (§ 3 Abs. 4 S. 2 Nr. 5 BDSG) und damit ein im Ansatz rechtfertigungsbedürftiger Vorgang vorliegen (§ 4 Abs. 1 BDSG).

⁷⁴⁴ Gola/Schomerus, BDSG, § 3 Rdnr. 43; Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 198; Metschke/Wellbrock, Datenschutz in Wissenschaft und Forschung, Abschnitt 3.3, S. 20. S. auch oben Kap. 1.2, S. 11ff.

⁷⁴⁵ Zu diesem relativen Ansatz des Personenbezug s. oben S. 12ff.

⁷⁴⁶ So Gola/Schomerus, BDSG, § 3 Rdnr. 43, was auch zu konsistenten Ergebnissen im Vergleich mit der Bewertung der Löschung personenbezogener Daten führt, s.o. S. 36f. Anderer Ansicht: Metschke/Wellbrock, Datenschutz in Wissenschaft und Forschung, Abschnitt 3.3, S. 20.

⁷⁴⁷ Zu den Methoden der Anonymisierung, zu denen neben der (zwingenden) Entfernung der unmittelbaren Identifikatoren insbesondere auch die Löschung weiterer Daten, das Aggregieren sowie das bewusste Einstreuen von Störgrößen bzw. Zufallsfehlern gehört: Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 205ff.

⁷⁴⁸ Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129; Gola/Schomerus, BDSG, § 3 Rdnr. 31. S.a. oben S. 36.

Im Übrigen könnte der grundsätzlich ebenfalls eine Erlaubnis erfordernde Auffangtatbestand des Nutzens vorliegen (§ 3 Abs. 5 BDSG).⁷⁴⁹

Allerdings ist das Ziel und der Effekt der Anonymisierung, dass der Personenbezug entfällt und damit auch die Anwendungsvoraussetzungen des Datenschutzrechts entfallen. Wenn mit der Anonymisierung der direkte Weg dorthin aus dem Datenschutzrecht heraus eingeschlagen wird, ohne dass dabei noch personenbezogene Daten für andere Zwecke „abgezweigt“ werden, dann muss aber nach Sinn und Zweck auch für den Vorgang des Anonymisierens das Verbot mit Erlaubnisvorbehalt (vgl. § 4 Abs. 1 BDSG) entfallen. Falls dieser Vorgang an eine besondere Erlaubnis gebunden wäre, würde der Zustand des Vorhaltens von personenbezogenen Daten, den das Datenschutzrecht grundsätzlich – wenn auch unter Erlaubnisvorbehalt – verbietet, perpetuiert, was widersinnig wäre.⁷⁵⁰ Ein nach dem Wortlaut des Datenschutzrechts vielleicht naheliegender oder zumindest noch möglicher Rechtfertigungsbedarf wäre gegebenenfalls vor dem Hintergrund des Zwecks des Datenschutzrechts teleologisch zu reduzieren, letztlich also abzulehnen.⁷⁵¹

7.3.2.2 Anforderungen an die Anonymisierung

Allerdings muss sich der Vorgang der Anonymisierung an dem Ziel ausrichten, tatsächlich den Personenbezug zu beseitigen, also eine Re-Identifizierung zu verhindern.⁷⁵² Häufig wird das Ziel einer absoluten Anonymität, also dass die Daten überhaupt nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können, nicht erreicht werden. Bei einer lediglich relativen (bzw. faktischen) Anonymität, bei welcher eine Zuordnung noch möglich ist, aber nur unter Einsatz eines unverhältnismäßigen Aufwandes an Zeit, Kosten und Arbeitskraft, bestehen allerdings noch Restrisiken einer Re-Identifizierung.

Es ist daher zu empfehlen, eine gewisse Risikoversorge beim Umgang mit faktisch anonymen Daten zu treffen.⁷⁵³ So könnten beispielsweise bestimmte technisch-organisatorische Sicherheitsmaßnahmen getroffen werden, vor allem gegen einen Datenzugriff von außen oder durch eine weitere Ausdünnung von Quasi-Identifikatoren, sofern der technische Fortschritt eine Re-Identifizierung mit der Zeit nennenswert erleichtern sollte.⁷⁵⁴ Beim Datenumgang nur durch den Behandler selbst dürfte sich das angezeigte Maß an Vorsorge aber in überschaubarem Rahmen halten.

Bei Übertragung faktisch anonymer Daten an andere Stellen sollten jedoch das bei diesen möglicherweise vorhandene Zusatzwissen oder sonstige Re-Identifizierungsmöglichkeiten eingeschätzt werden. Denn diese könnten zu einer Re-Identifizierbarkeit mit verhältnismäßigem Aufwand und damit dem Wiederaufleben des Personen-

⁷⁴⁹ Vgl. oben S. 37f.

⁷⁵⁰ Bei effektiv anonymisierten Daten droht keine Beeinträchtigung der Persönlichkeitsrechte des Einzelnen mehr, deren Schutz beim Umgang mit personenbezogenen Daten Zweck des Datenschutzrechts ist (prototypisch für das deutsche Recht: § 1 Abs. 1 BDSG). Außerdem würde andernfalls die Erfüllung der Zielvorgabe bzw. des Programmsatzes der Datenvermeidung und Datensparsamkeit, wie er u.a. in § 3a BDSG enthalten ist, unnötig erschwert.

⁷⁵¹ Vgl. zur ähnlichen Argumentation bei automatisierten Auswertungen mit lediglich anonymer Ausgabe (Kap. I.4), welche für die vollständige Anonymisierung erst recht gelten muss, oben S. 37ff. m.w.N.

⁷⁵² S. auch oben Kap. I.2, S. 17ff.

⁷⁵³ S. auch oben Kap. I.2, S. 23f.

⁷⁵⁴ Auch wenn diese Sicherheitsmaßnahmen keineswegs so umfassend sein müssen wie diejenigen nach den für personenbezogene Daten einschlägigen Datenschutzgesetzen (z.B. § 9 BDSG), welche für faktisch anonyme Daten nicht direkt gelten. Eine gewisse Orientierung an den entspr. Regelungen bietet sich gleichwohl an.

bezugs sowie letztlich dem Vorliegen einer Rechtfertigungsbedürftigen Übermittlung führen.⁷⁵⁵ Eine entsprechende Einschätzung sollte auch die empfangende Stelle vornehmen, damit sich aus einer möglichen Zusammenführung mit bei ihr bereits vorhandenen Datenbeständen kein doch wieder personenbezogener Datenumgang ergibt. Die übertragende Stelle könnte sich durch vertragliche Verpflichtungen des Datenempfängers weiter absichern, welche Re-Identifizierungsverbote und gewisse technisch-organisatorische Schutzmaßnahmen einschließen.⁷⁵⁶

Abschließend bleibt hier aber festzuhalten, dass auch für den Umgang mit faktisch anonymen Daten kein Verbot mit Erlaubnisvorbehalt besteht.

7.4 Verwendung von Behandlungsdaten in pseudonymisierter Form durch nicht behandelndes Personal in der gleichen Fachabteilung



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in pseudonymisierter Form an nicht behandelndes Personal in der gleichen Fachabteilung für Zwecke der Forschung oder Qualitätssicherung übermittelt werden?

7.4.1 Personenbezogene Datenverwendung der Behandlungseinrichtung

Aufgrund der Pseudonymisierung stellt sich zunächst die Frage, ob für das nicht behandelnde Personal überhaupt ein Personenbezug vorliegt. Wenn das nicht behandelnde Personal keinen Zugriff auf die Zuordnung des Pseudonyms zur Person des Patienten hat, dann ließe sich auf Basis der Relativität des Personenbezugs vertreten, dass dieses Personal keine personenbezogenen Daten mehr verwendet.⁷⁵⁷

Allerdings wird der Personenbezug in aller Regel, auch wenn man dessen Relativität unterstellt, auf eine verantwortliche Stelle in ihrer Gesamtheit bezogen. So gesehen liegt auf die jeweilige Behandlungseinrichtung bezogen, ein Verwenden personenbezogener Daten vor, für welches diese verantwortlich ist, auch wenn das im Einzelnen eingesetzte Personal den Personenbezug nicht (ohne Weiteres) herstellen kann. Es genügt, wenn die verantwortliche Stelle die Möglichkeit hat, über das Weisungsrecht allen ihren Mitarbeitern gegenüber letztlich den Personenbezug herzustellen.

Die Pseudonymisierung stellt vor diesem Hintergrund lediglich eine technisch-organisatorische Maßnahme der Datensicherheit dar, die zudem teils – vor allem für die Forschung – durch besondere datenschutzrechtliche Pflichten angeordnet wird. Sie schließt jedoch nicht den Personenbezug und damit den grundsätzlichen datenschutzrechtlichen Erlaubnisvorbehalt für die Datenverwendung aus.

⁷⁵⁵ Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 211; Gola/Schomerus, BDSG, § 3 Rdnr. 44a.

⁷⁵⁶ Denkbar, wenn auch weniger wichtig, wäre eine interne Selbstbindung hinsichtlich der Verwendungszwecke (z.B. für die wissenschaftliche Forschung im Allgemeinen), welche auch auf den Datenempfänger erstreckt werden könnte.

⁷⁵⁷ Zu diesem Ansatz s. oben S. 12ff.

7.4.2 Kein besonders rechtfertigungsbedürftiges Übermitteln, aber rechtfertigungsbedürftige sonstige Verwendung

Ein Übermitteln ist nach allgemeinem Datenschutzrecht die Weitergabe von personenbezogenen Daten an einen Dritten außerhalb der ursprünglich verantwortlichen Stelle, wozu das nicht behandelnde Personal der gleichen Fachabteilung aber noch nicht zählt. Nach den Krankenhausgesetzen mancher Bundesländer wird die (technische) Datenübertragung zwischen Fachabteilungen einer Klinik auch als Übermittlung gewertet, was aber als Ausnahme zum allgemeinen Datenschutzrecht keineswegs auf nicht behandelndes Personal in derselben Fachabteilung übertragen werden kann, zumal wenn dieses nur Zugang zu pseudonymisierten Daten erhält.

Jedenfalls dürfte aufgrund der Pseudonymisierung keine Kenntnisnahme vom Personenbezug durch das nicht behandelnde Personal erfolgen oder möglich sein und damit letztlich auch kein Offenbaren im Sinne der Schweigepflicht nach § 203 StGB vorliegen.⁷⁵⁸ Voraussetzung ist freilich, dass das nicht behandelnde Personal vom behandelnden Personal, der IT-Administration oder der Klinikleitung keinen Zugriff auf die Zuordnung des Pseudonyms zum Patienten erhält;⁷⁵⁹ die zuletzt Genannten müssen insoweit ausschließlich als Gehilfen des behandelnden Personals fungieren. Diese Anforderungen dürften gerade innerhalb einer Fachabteilung nicht ganz einfach zu erfüllen sein, ausgeschlossen ist dies aber nicht. Deshalb kommt es insoweit mangels Offenbaren nicht darauf an, ob und inwieweit sich aus der Schweigepflicht auch Schranken innerhalb einer Fachabteilung ergeben.⁷⁶⁰

Auch wenn, unabhängig von den datenschutzrechtlichen Regeln, zwischen verschiedenen Fachabteilungen, von denen mindestens eine nicht in das Behandlungsgeschehen involviert ist, innerorganisatorische Schranken aufgrund der Schweigepflicht greifen können, so dürfte doch hier aufgrund der Pseudonymisierung keine Kenntnisnahme vom Personenbezug und auch keine reguläre Möglichkeit dazu, letztlich also kein Offenbaren im Sinne des § 203 StGB vorliegen.⁷⁶¹ Voraussetzung ist freilich, dass das Personal der nicht behandelnden Fachabteilung von der behandelnden Abteilung, der IT-Administration oder der Klinikleitung keinen Zugriff auf die Zuordnung des Pseudonyms zum Patienten erhält;⁷⁶² diese müssen insoweit ausschließlich als Gehilfen der behandelnden Fachabteilung fungieren.

758 Vgl. hierzu und zum Erfordernis einer gewissen Offenkundigkeit des Personenbezugs für ein Offenbaren oben Kap. I.4.2.1.2, S. 48ff., und unten Kap. I.8.1.3, S. 262ff.

759 Gleiches gilt, um eine Re-Identifizierung durch Mustervergleich auszuschließen, in Bezug auf den Zugriff auf (zumindest nennenswerte Teile von) dessen personenbezogenen Behandlungsdaten, was aber in aller Regel ohnehin eine Mitbehandlung voraussetzt.

760 Zur Frage der innerorganisatorischen Schweigepflicht bzw. Offenbarung in der PKV: Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für private Krankenversicherer, insbesondere bei der innerorganisatorischen Geheimnisweitergabe, zusammenfassend auf S. 250: „Eine innerorganisatorische Geheimnisweitergabe unter Schweigepflichtigen ist dann kein Offenbaren i.S.d. § 203, wenn die Daten zu einem Zweck weitergegeben werden, der der Eigenart der jeweiligen Sonderverbindung zwischen Geheimnisschützten und Schweigepflichtigen bzw. der dahinter stehenden Organisation entspricht“. Dem entspricht die Herausnahme von Datenweitergaben zwischen behandelndem Personal innerhalb eines Krankenhauses zu Behandlungszwecken aus dem Offenbarungsbegriff bzw. der gegenseitigen Schweigepflicht. Folgt man der im Ansatz jedenfalls überzeugenden Argumentation von Köpke, dürfte jedoch die Weitergabe von nicht effektiv pseudonymisierten Behandlungsdaten zur Sekundärnutzung für andere Zwecke ein rechtfertigungspflichtiges Offenbaren darstellen.

761 Vgl. hierzu und zum Erfordernis einer gewissen Offenkundigkeit des Personenbezugs für ein Offenbaren oben Kap. I.4.2.1.2, S. 48ff., und unten Kap. I.8.1.3, S. 262ff.

762 Gleiches gilt, um eine Re-Identifizierung durch Mustervergleich auszuschließen, in Bezug auf den Zugriff auf (zumindest nennenswerte Teile von) dessen personenbezogenen Behandlungsdaten, was aber in aller Regel ohnehin eine Mitbehandlung voraussetzt.

Gleichwohl liegt aber – für die Gesamtorganisation – eine rechtfertigungsbedürftige sonstige Verwendung personenbezogener Daten vor. Die Übertragung an nicht behandelndes Personal würde dabei auch innerorganisatorisch, wenn auch ohne Übermittlung zu sein, einen erhöhten Rechtfertigungsbedarf auslösen, der allerdings durch die Pseudonymisierung wieder kompensiert wird. Letztlich liegt damit ein Rechtfertigungsbedarf wie beim unveränderten Umgang durch behandelndes Personal vor, wobei hier zu beachten ist, dass Pseudonymisierungspflichten erfüllt wurden.

7.5 Verwendung von Behandlungsdaten in pseudonymisierter Form durch Personal anderer Fachabteilungen



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in pseudonymisierter Form an Personal anderer Fachabteilungen desselben Krankenhauses für Zwecke der Forschung oder Qualitätssicherung übermittelt werden?

7.5.1 Personenbezogene Datenverwendung der Behandlungseinrichtung

Für die gesamte Behandlungseinrichtung als verantwortliche Stelle liegt grundsätzlich Personenbezug vor, auch wenn dieser für das nicht behandelnde Personal anderer Fachabteilungen aufgrund der Pseudonymisierung nicht ohne Weiteres herstellbar ist. Die Pseudonymisierung dient dabei als technisch-organisatorische Sicherheitsmaßnahme und der Erfüllung spezifischer Pflichten, vor allem im Bereich der Forschung.

7.5.2 Teils besonders rechtfertigungsbedürftiges Übermitteln, teils rechtfertigungsbedürftige sonstige Verwendung

Wie bereits ausgeführt, ist ein Übermitteln nach allgemeinem Datenschutzrecht die Weitergabe von personenbezogenen Daten an einen Dritten außerhalb der ursprünglich verantwortlichen Stelle, hier also der Behandlungseinrichtung. Zur Behandlungseinrichtung zählen aber auch andere (nicht behandelnde) Fachabteilungen und deren Personal. Damit liegt in der vorliegenden Konstellation grundsätzlich kein besonders rechtfertigungsbedürftiges Übermitteln vor. Insoweit kann auf die Ausführungen zur Rechtfertigung der internen Datenverwendung durch Behandler in pseudonymisierter Form verwiesen werden.

Allerdings ordnen die bereichsspezifischen Regeln mancher Bundesländer zum Datenschutz im Krankenhaus abweichend von diesem allgemeinen Grundsatz für die (technische) Datenübertragung (einschließlich der Gewährung von Zugriffsrechten) zwischen Fachabteilungen einer Klinik die entsprechende Geltung der Übermittlungsvorschriften an oder werten die innerorganisatorische Übertragung als Übermittlung mit der Folge, dass diese prinzipiell denselben strengen Regeln wie die Weitergabe an komplett außenstehende Dritte genügen muss. Dies wird in folgenden

Normen generell für alle Weitergaben zwischen Fachabteilungen bzw. internen Organisationseinheiten für alle Zwecke oder zumindest alle Zwecke außer den besonders ausgenommenen (wie solchen der Behandlung) angeordnet:

- Bremen: § 3 Abs. 2 S. 1 KHDSG HB
- Hessen: § 12 Abs. 3 LKHG HE
- Mecklenburg-Vorpommern: § 34 Abs. 3 LKHG MV
- Nordrhein-Westfalen: § 5 Abs. 1 S. 2 GDSG NW (sofern nicht unmittelbar in Behandlung involviert)
- Saarland: § 13 Abs. 3 S. 1 LKHG SL (sofern nicht zur Behandlung oder sozialen Betreuung erforderlich)
- Evangelische Kirche: § 3 Abs. 2 DSVO
- Katholische Kirche: § 3 Abs. 2 PatDSO

In all diesen Fällen sind die jeweiligen Übermittlungsschranken auch bei der fachabteilungsübergreifenden Forschung mit für die Gesamteinrichtung noch personenbezogenen, wenn auch für einzelne Abteilungen möglicherweise nur pseudonymen Daten zu beachten.⁷⁶³

Zudem differenzieren die Forschungsklauseln der LKHG bezogen auf den Forschungszweck häufig nach privilegierter fachabteilungsinterner Eigenforschung auf der einen und der Forschung durch andere Fachabteilungen oder gar Außenstehende auf der anderen Seite, ohne dass hiermit eine generelle Gleichstellung von fachabteilungsübergreifender Datenweitergabe und Datenübermittlung an Dritte verbunden wäre. Die entsprechenden Klauseln können Übersicht 2 entnommen werden.⁷⁶⁴

Im Rahmen eines eventuellen Auslegungs-, Anwendungs- bzw. Abwägungsspielraums, den die (entsprechend anwendbaren) Übermittlungsvorschriften lassen, wird man allerdings eine innerorganisatorische Übermittlung eher rechtfertigen können als die Weitergabe an eine eigenverantwortliche dritte Stelle. Dies gilt zumal bei vorgängiger Pseudonymisierung, die zwischen Fachabteilungen zudem wohl effektiver umgesetzt werden kann als innerhalb einer Abteilung. Wenn allerdings für die hier relevanten Zwecke der Qualitätssicherung oder Forschung überhaupt keine Übermittlungsbefugnis bestünde, käme in den genannten Ländern auch keine Übertragung zwischen Fachabteilungen in Betracht. Jedoch gestatten alle diese fünf Länder, wenn auch unter bestimmten Bedingungen, die Übermittlung zu Zwecken der Qualitätssicherung und Forschung.

Auch wenn, unabhängig von den datenschutzrechtlichen Regeln, zwischen verschiedenen Fachabteilungen, von denen mindestens eine nicht in das Behandlungsgeschehen involviert ist, innerorganisatorische Schranken aufgrund der Schweigepflicht greifen können, so dürfte doch hier aufgrund der Pseudonymisierung keine Kenntnisnahme vom Personenbezug und auch keine reguläre Möglichkeit dazu, letztlich also kein Offenbaren im Sinne des § 203 StGB vorliegen.⁷⁶⁵ Voraussetzung ist freilich, dass das Personal der nicht behandelnden Fachabteilung von der behandeln-

763 Die Erstreckung der Übermittlungsschranken führt wohl im Gegensatz zur Lage bei rechtlich gänzlich eigenverantwortlichen Dritten nicht dazu, dass die pseudonymen Daten für interne Abteilungen, die nicht über die Zuordnungsfunktion verfügen, nicht mehr als personenbezogen gelten.

764 S. oben S. 87ff.

765 S. auch soeben S. 221f. Vgl. hierzu und zum Erfordernis einer gewissen Offenkundigkeit des Personenbezugs für ein Offenbaren oben Kap. I.4.2.1.2, S. 48ff., und unten Kap. I.8.1.3, S. 262ff.

den Abteilung, der IT-Administration oder der Klinikleitung keinen Zugriff auf die Zuordnung des Pseudonyms zum Patienten erhält;⁷⁶⁶ die zuletzt Genannten (IT-Administratoren, Klinikverwaltung) müssen insoweit ausschließlich als Gehilfen der behandelnden Fachabteilung fungieren.

⁷⁶⁶ Gleiches gilt, um eine Re-Identifizierung durch Mustervergleich auszuschließen, in Bezug auf den Zugriff auf (zumindest nennenswerte Teile von) dessen personenbezogenen Behandlungsdaten, was aber in aller Regel ohnehin eine Mitbehandlung voraussetzt.