Datenschutz in der Rehabilitationsforschung*

Data Protection in Rehabilitation Research

Autoren A.-K. Exner[1], H. Gerold[2], J. Breckenkamp[1], J. Bahmer[3], R. Klemke[4], G. Berg-Beckhoff[5], A. Horschke[3], O. Razum[1]

Institute Die Institutsangaben sind am Ende des Beitrags gelistet

Schlüsselwörter
- Datenschutz
- Rehabilitation
- informierte Einwilligung

Key words
- data protection
- rehabilitation
- informed consent

Zusammenfassung

Der Datenschutz ist in Gesetzen festgelegt und muss von der Wissenschaftlerin/dem Wissenschaftler eingehalten werden. In dieser Übersicht wird aufgezeigt, an welchen Stellen in der Rehabilitationsforschung datenschutzrelevante Aspekte berücksichtigt werden müssen. Dabei sind das Sozialgesetzbuch X, das Bundesdatenschutzgesetz und die jeweiligen Landesdatenschutzgesetze wichtige Quellen. Für die Forschungspraxis mit Studienteilnehmenden werden konkrete Empfehlungen gegeben, was eine Patienteninformation und eine Einwilligungserklärung beinhalten sollte. Die Erhebung, Verarbeitung, Nutzung, Speicherung, Veröffentlichung und Archivierung von personenbezogenen Forschungsdaten unter Berücksichtigung der Vorgaben des Datenschutzes wird erläutert. Ein Beispiel aus der Praxis (siehe online unter www.thieme-connect.de/ejournals/toc/rehabilitation) zeigt, wie mithilfe eines externen Datentreuhänders durch eine Abtrennung der personenbezogenen Daten die Forschungsdaten pseudonymisiert bzw. anonymisiert werden können.

Abstract

Data protection is regulated by legislation and has to be adhered to by scientists, too. This overview shows where aspects of data protection have to be considered in rehabilitation research. Important legal sources are the code of social law X, the German Federal Data Protection Act and the data protection acts of the German states. Specific recommendations about patient information sheet and written informed consent are given for research based on interviews with study participants. Furthermore, operations such as collecting, processing, using, storing, publishing and archiving of personal data are explained, taking into account the requirements of data protection. A practical example (URL: www.thieme-connect.de/ejournals/toc/rehabilitation) shows how to separate personal data and research data using the services of an external data custodian.

Bibliografie
DOI http://dx.doi.org/10.1055/s-0033-1357115
Online-Publikation: 20.12.2013
Rehabilitation 2014; 53: 258–267
© Georg Thieme Verlag KG Stuttgart · New York
ISSN 0034-3536

Korrespondenzadresse
Anne-Kathrin Exner
Fakultät für Gesundheitswissenschaften
AG3 Epidemiologie & International Public Health
Universität Bielefeld
Universitätsstraße 25
33615 Bielefeld
anne-kathrin.exner@uni-bielefeld.de

Einleitung

Unter Datenschutz wird der vertrauliche Umgang mit personenbezogenen Daten (→ Glossar, siehe online unter www.thieme-connect.de/ejournals/toc/rehabilitation) verstanden. Tatsächlich geht es um die Wahrung der Persönlichkeitsrechte von Menschen. Jeder soll grundsätzlich selbst bestimmen können, wem oder an welcher Stelle er welche Daten über sich mitteilt oder verschweigt (sog. abgeleitetes Grundrecht auf „informationelle Selbstbestimmung“) (Bundesverfassungsgericht 65/1). Das informationelle Selbstbestimmungsrecht (abgeleitet aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz – GG) und die Freiheit der Forschung (Art. 5 Abs. 3 GG) treffen bei Forschungsprojekten aufeinander. Zwischen diesen teilweise konkurrierenden Grundrechten sollte durch eine sorgfältige Planung des Forschungsprojektes im Konfliktfall ein schonender Ausgleich geschaffen werden. Zum Beispiel könnte die Zahl der zu erhebenden Variablen möglichst gering gehalten und die Anonymität der Ergebnisdaten erreicht werden, ohne dadurch das Forschungsziel zu gefährden.

*Koordinatoren der Reihe „Methoden in der Rehabilitationsforschung“: Prof. Dr. Dr. Hermann Faller, Würzburg; Prof. Dr. Thomas Kohlmann, Greifswald; Prof. Dr. Dr. Christian Zwingmann, Bochum; Interessenten, die einen Beitrag zur Reihe beisteuern möchten, werden gebeten, vorab Kontakt aufzunehmen christian.zwingmann@web.de

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Der Datenschutz ist durch Gesetze geregelt. Je nach Datenquelle (→ Glossar), z. B. Sozialversicherung oder Befragung, aus der Forschungsdaten erhoben werden sollen, sind unterschiedliche Gesetze zu beachten, die sich im Detail unterscheiden können. Eine Struktur gibt es in Form sog. Datenschutzgrundsätze. Dazu gehören das Verbot mit Erlaubnisvorbehalt, die Grundsätze der Datenvermeidung, der Zweckbestimmung und der Zweckbindung, der Datensparsamkeit, der Erforderlichkeit, der Direkterhebung und der Transparenz. Sie ziehen sich wie ein roter Faden durch alle Datenschutzgesetze. Wer in der Forschung sein Datenschutzmanagement an diesen Grundsätzen ausrichtet, kommt zu praktikablen Lösungen – selbst wenn die genaue Rechtsgrundlage zunächst unbekannt ist. Das entbindet die Wissenschaftlerin/den Wissenschaftler jedoch nicht davon, sich in der Projektplanung mit den spezifischen Datenschutzvorschriften zu befassen, die für die Datenquellen gelten, aus denen die Daten erhoben werden sollen. Die datenschutzrechtliche Verantwortung liegt immer bei der Person oder Stelle, die für eigene Zwecke (Aufgaben), wie bspw. die Forschung, personenbezogene Daten verarbeitet. Bestimmte Aspekte des Datenschutzes sind weitgehend identisch mit den Ethik-Grundsätzen der Deklaration von Helsinki des Weltärztebundes [1].

In diesem Artikel wird dargestellt, welche datenschutzrelevanten Aspekte in einem Reha-Forschungsprojekt berücksichtigt werden müssen. Zunächst werden allgemeine Begriffsbestimmungen gegeben und die Datenschutzgrundsätze erklärt. Im Anschluss werden die Struktur der deutschen Datenschutzgesetze sowie die Arbeitsschritte für die Datenverarbeitung dargestellt. Datenschutzrelevante Aspekte bei der Nutzung von personenbezogenen Daten für die Forschung werden erläutert. Dazu wird zunächst die Gestaltung eines Projektes beschrieben, das mit anonymen Daten arbeitet, sowie eine Befragung, bei der eine informierte Einwilligung (→ Glossar) zur Studienteilnahme erforderlich ist. Weiterhin wird auf die Einbeziehung weiterer Datenquellen, insbesondere von Sozialdaten (→ Glossar), eingegangen. Der Umgang mit Forschungsdaten, deren Veröffentlichung und Archivierung sowie die „Rechtsfolgen bei Verstößen" gegen den Datenschutz werden erläutert. Anhand eines Beispiels aus der Rehabilitationspraxis (siehe online unter www.thieme-connect.de/ejournals/toc/rehabilitation) wird dargestellt, wie mithilfe eines externen Datentreuhänders (→ Glossar) Forschungsdaten räumlich getrennt von personenbezogenen Daten gelagert werden.

Allgemeine Begriffsbestimmungen

▼

Personenbezogene Daten

Als personenbezogene oder personenbeziehbare Daten (→ Glossar) gelten Informationen, die einer Person zugeordnet sind oder die eine Zuordnung zu einer Person einfach ermöglichen, z. B. durch Kombination bekannter Merkmale oder über ein Zuordnungskriterium (auch Pseudonym [→ Glossar] genannt) (**Tab. 1**). „Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben" (§ 67 Abs. 12 Sozialgesetzbuch – SGB X und § 3 Abs. 9 Bundesdatenschutzgesetz – BDSG). Liegen personenbezogene oder personenbeziehbare Daten vor, müssen die Datenschutzgesetze eingehalten werden. Wenn im Weiteren von personenbezogenen Daten gesprochen wird, sind auch personenbeziehbare Daten gemeint.

Anonyme Daten

Im Gegensatz zu personenbezogenen Daten können absolut anonyme Daten keiner Person zugewiesen werden. Faktisch anonyme Daten können nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person (→ Glossar) zugeordnet werden. Bei faktisch oder absolut anonymen Daten sind daher keine Datenschutzgesetze zu beachten (**Tab. 1**).

Verantwortliche Stelle

Alle Stellen und Personen, die bei ihrer Arbeitserledigung in Wirtschaft, Verwaltung oder Forschung mit personenbezogenen Daten umgehen, sind selbst für den Datenschutz verantwortlich (siehe Begriff „verantwortliche Stelle" [→ Glossar]). Die Verpflichtung ergibt sich aus den Gesetzen und findet in Begriffen wie Datengeheimnis (→ Glossar), Sozialgeheimnis (→ Glossar) oder Arztgeheimnis (→ Glossar) seinen Niederschlag.

Datenschutzgrundsätze

▼

Verbot mit Erlaubnisvorbehalt

Nach dem Verbot mit Erlaubnisvorbehalt ist es zunächst verboten, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Dies ist nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG), die jeweiligen Landesdatenschutzgesetze (LDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Jeder Verantwortliche muss den gesetzlichen Vorgaben entsprechend und vertraulich mit personenbezogenen Daten umgehen. Auch die Arbeitsumgebung muss so gestaltet werden, dass personenbezogene Daten nur Berechtigten zugänglich sind. Verantwortliche dürfen die personenbezogenen Daten insbesondere nicht Unbefugten mitteilen. Unbefugte sind alle, die nicht zum wissenschaftlichen Team gehören (§ 67 SGB X und § 4 BDSG).

Grundsatz der Datenvermeidung

Bei der Erhebung von Daten gilt der Grundsatz der Datenvermeidung (§ 78b SGB X und § 3a BDSG). Dieser zielt darauf, den Personenbezug von Anfang an zu vermeiden. Allerdings sind Forschungsprojekte selten, die ohne personenbezogene Daten auskommen. In der Praxis ist es üblich, dass Wissenschaftlerinnen und Wissenschaftler zumindest zeitweise mit personenbezogenen Daten umgehen. Zum Beispiel werden die Forschungsdaten aus Krankenblattakten oder anderen Datenquellen entnommen, die den Namen deutlich lesbar enthalten. Oder es sollen Studienteilnehmerinnen und -teilnehmer zu mehreren Zeitpunkten befragt werden. Die Wissenschaftlerinnen und Wissenschaftler benötigen hier Namen und Kontaktdaten, um die Fragebogen an die Postanschrift zu schicken. Eine Möglichkeit Unterlagen zu versenden, ohne Adressen zu speichern, ist das Adressmitteilungsverfahren. Bei diesem Verfahren werden Institutionen, Behörden oder Einrichtungen, die Adressen verwalten, frankierte Umschläge und das zu versendende Material gegeben. Die Adressverwalter adressieren die Umschläge und verschicken die Unterlagen per Post [2] (s. Beispiel aus der Rehabilitationspraxis online unter www.thieme-connect.de/ejournals/toc/rehabilitation).

Grundsatz der Zweckbestimmung und Zweckbindung

Eine „zweckfreie" Erhebung personenbezogener Daten ist verboten (Vorratsdatenspeicherung). Bei jeder Erhebung muss

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Tab. 1 Kategorisierung oder Abstufung personenbezogener, personenbeziehbarer, faktisch anonymer und absolut anonymer Daten.

Daten-Kategorie	Eigenschaft	Beispiel	Gesetz anwendbar?
personenbezogen	Name und Identifizierungsdaten sind vorhanden	Karl Mustermann äußerte sich im Jahr 2004 erstmals zu seiner Krebserkrankung.	ja Bezogen auf dieses Beispiel ist es zulässig, alles zu berichten und zu verarbeiten, was der Betroffene selbst mitteilt (Einwilligung).
pseudonym personenbeziehbar	Daten sind einem Pseudonym zugeordnet. Über eine Zuordnungsliste kann der Verantwortliche den Pseudonymen den Namen leicht zuordnen (Telefonnummer, Versicherungsnummer, Patientennummer, Stimme...).	Proband 08–15 beantwortete die Frage nach dem Familieneinkommen mit der Kategorie „zwischen 50 000 und 60 000 EUR". Die Aussage ist zuordenbar, solange die Zuordnungsliste existiert. Ebenfalls zuordenbar wäre die Aussage: Der Bundeskanzler des Jahres 1972 (Willy Brandt).	ja
faktisch anonym	Name und Identifikationsdaten sind gelöscht. Zuordnung der Daten zu einem Namen ist gar nicht oder nur mit großem Aufwand an Zeit, Kosten und Arbeitskraft möglich. Es gibt keine Zuordnungsliste mehr.	Ein männlicher Proband (60 Jahre) beantwortete die Frage nach dem Familieneinkommen mit der Kategorie „zwischen 50 000 und 60 000 EUR".	nein
absolut anonym	Es gibt keine Namen und Identifizierungsdaten, die eine Zuordnung zu einer Person ermöglichen würden.	Unter den 60-jährigen männlichen Befragungsteilnehmern haben immerhin 47 % die Frage nach dem Familieneinkommen mit der Kategorie „zwischen 50 000 und 60 000 EUR" beantwortet.	nein

vorab konkret festgelegt sein, für welche Zwecke die Daten verwendet werden sollen, denn nur so kann gewährleistet werden, dass der Umgang mit den Daten in einem überschaubaren Rahmen bleibt (siehe auch Grundsatz der Datensparsamkeit). Die Zweckbestimmung schließt eine Zweckbindung ein. Das bedeutet, einmal erhobene Daten dürfen nur für die festgelegten Zwecke verwendet werden. Diese dürfen nur (weiter) verwendet werden, wenn ein Gesetz das zulässt oder der Betroffene ausdrücklich eingewilligt hat (Zweckänderung) (§ 14 Abs. 2, § 28 Abs. 2 oder Abs. 5 BDSG). Die Zweckbindung gilt für die erhobenen Primärdaten (→ Glossar) bis zu deren Löschung. Selbst wenn der Personenbezug aufgehoben wird (Anonymisierung), dürfen die Primärdaten aus forschungsethischer Sicht nicht für andere Forschungsprojekte verwendet werden.

Grundsatz der Datensparsamkeit

Datensparsamkeit (auch: Erforderlichkeit) gibt vor, so wenig personenbezogene Daten wie möglich zu verarbeiten und nur diejenigen personenbezogenen Daten zu erheben, die zur Beantwortung der Forschungsfrage unbedingt erforderlich sind (§ 78b SGB X und § 3a BDSG). Vor der Erhebung muss der Datenkatalog festgelegt und sachlich begründet werden. Dabei muss die Angemessenheit und Eignung der Daten zur Untersuchung der Fragestellung durch die Wissenschaftlerinnen und Wissenschaftler geprüft werden. Hierzu gehören auch forschungs- oder medizinethische Fragestellungen zur Zumutbarkeit an die Probandinnen und Probanden, welche durch die Ethikkommission geprüft werden. Eine Ausweitung des Katalogs nach Beginn der Datenerhebung ist nur zulässig, wenn dadurch die Zweckbestimmung des Forschungsprojekts nicht geändert wird. Falls bspw. im Rahmen eines Pretests festgestellt wird, dass eine Frage anders zu formulieren oder ein bestimmter Aspekt genauer zu hinterfragen ist, kann der finale Fragebogen (=Datenkatalog) noch angepasst werden. Eine unzulässige Erweiterung der geplanten Datenerhebung wäre dagegen, zusätzliche Daten aus anderen Quellen wie Krankenblattakte oder Rehabilitationsentlassungsbericht zu entnehmen oder Informationen vom Hausarzt zu erfragen, ohne dies vorher in der Teilnehmerinformation zu beschreiben (siehe Abschnitt Teilnehmerinformation und Einwilligungserklärung). Eine solche Erweiterung der Zweckbestimmung der Forschungsdaten ist nur zulässig, wenn eine erneute Einwilligung der Teilnehmer eingeholt wird. Ein Beispiel für die (Nicht-)Erforderlichkeit von personenbezogenen Angaben ist das Geburtsdatum von Studienteilnehmern. Aus datenschutzrechtlicher Sicht genügt das Geburtsjahr, wenn das Alter nicht exakt auf Tag und Monat berechnet werden muss.

Grundsatz der Direkterhebung und Transparenz

Daten über eine Person sollen grundsätzlich bei dieser erhoben werden (Direkterhebungsgrundsatz). Dabei muss der Person gegenüber angegeben werden, welche Stelle die Daten wofür benötigt (Zweckbestimmung) und an welche anderen Stellen die Daten weitergegeben werden, wie lange und aus welchem Grund sie gespeichert werden (Grundsatz der Transparenz) (§ 4 BDSG) (siehe auch Teilnehmerinformation und -einwilligung).

Datenverarbeitung

In einem Forschungsvorhaben mit personenbezogenen Daten müssen nach dem Sozialdatenschutz (geregelt im SGB X) und dem BDSG mehrere Arbeitsschritte beachtet werden: das Erheben, das Verarbeiten und das Nutzen der Daten. Durch diese

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Definitionen sind bei jeder denkbaren, personenbeziehbaren Datenverwendung die Datenschutzgesetze zu beachten.

- „Erheben" ist das Beschaffen personenbezogener Daten – hierbei sind die Datenschutzgrundsätze zu beachten (§ 67 Abs. 5 SGB X, § 3 Abs. 3 BDSG).
- „Verarbeiten" ist das Speichern, womit jede Form der Aufbewahrung in Papier, Zeichen, Bild, Ton oder elektronischer Form gemeint ist. Verarbeiten ist auch das Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 67 Abs. 6 SGB X, § 3 Abs. 4 BDSG).
- „Nutzen" ist jede Verwendung personenbezogener Daten, die nicht durch die Begriffe Erheben oder Verarbeiten erfasst wird (§ 67 Abs. 7 SGB X, § 3 Abs. 5 BDSG).

Rechtsvorschriften

Seit 1995 gibt es auf Ebene der Europäischen Union die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (95/46/EG)[1]. Dort ist festgelegt, welche Mindeststandards des Datenschutzes in den Mitgliedsländern geregelt sein müssen. Die Richtlinie dient einerseits der „Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten" zwischen den Mitgliedstaaten[2] und versucht andererseits, der Verarbeitung personenbezogener Daten enge Grenzen zu setzen: „Die Mitgliedsstaaten gewährleisten […] den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten" (Artikel 1 Abs. 1, 95/46/EG). Ausnahmeregelungen greifen, wenn die betroffene Person der Verarbeitung persönlicher Daten zugestimmt hat, oder aus Gründen öffentlichen Interesses (→ Glossar). In Deutschland gibt es eine große Anzahl Datenschutzgesetze wie der Sozialdatenschutz (SGB X), das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze. Hierbei gilt das sog. Subsidiaritätsprinzip: Wenn für bestimmte Anwendungsgebiete spezielle Datenschutzregelungen erlassen wurden, müssen diese beachtet werden. Gib es keine Spezialregelungen, gelten die allgemeinen Datenschutzgesetze.

Das deutsche Datenschutzrecht unterscheidet privatwirtschaftliche von öffentlich-rechtlichen Stellen, also Unternehmen und Betriebe auf der einen und öffentliche Verwaltungen auf der anderen Seite. Wenn es für die Tätigkeitsfelder der jeweiligen Betriebe oder Verwaltungen spezielle Datenschutzregelungen gibt, gelten diese. Für alle Sozialleistungsträger wie gesetzliche Krankenkassen, gesetzliche Unfallversicherungsträger oder Träger der gesetzlichen Rentenversicherung gelten die Spezialregelungen im Sozialdatenschutz. Für private Krankenversicherungen oder sonstige privatrechtliche Unternehmen gelten Bestimmungen des BDSG.

Öffentliche Verwaltungen der Länder oder Kommunen müssen die LDSG beachten. Das gilt auch für Körperschaften und Anstalten im Rechtskreis des Landes, es sei denn, sie wenden Bundesrecht an, für das Spezialgesetze gelten wie das SGB (z. B. Rentenversicherungsträger auf Landesebene). Auch gibt es Spezialgesetze der Länder wie das Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen im Land Nordrhein-Westfalen (Gesundheitsdatenschutzgesetz – GDSG NRW), welches wiederum als bereichsspezifische Regelung vorrangig vor dem LDSG NRW zu beachten ist. Wenn Forschungsdaten in diese gesetzliche Regelung fallen, so muss das GDSG NRW angewandt werden.

[1] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.
[2] Ziffer 8 der Gründe zum Erlass der Richtlinie 95/46/EG: URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.

Ansprechpartner zum Datenschutz

Ansprechpartner bei Fragen zum Datenschutz sind auf den verschiedenen Ebenen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Landesbeauftragten für Datenschutz (und Informationsfreiheit) und die betrieblichen und behördlichen Datenschutzbeauftragten. Bei jedem Projekt empfiehlt es sich, einen Datenschutzexperten bereits in die Planung einzubeziehen. Die Wissenschaftlerin/der Wissenschaftler sollte sich dazu an den Datenschutzbeauftragten des eigenen Instituts oder derjenigen Stellen wenden, bei denen sie ihre Daten aus personenbezogenen Datenquellen erheben wollen. Eine gesetzliche Verpflichtung hierzu besteht allerdings nicht.

Erhebung von Primärdaten in der Rehabilitationsforschung

Bei einem Forschungsvorhaben, bei dem Primärdaten erhoben werden, muss sich aus datenschutzrechtlicher Sicht die Wissenschaftlerin/der Wissenschaftler zunächst fragen, ob zu irgendeinem Zeitpunkt personenbezogene Daten, wie z. B. der Name oder Kontaktdaten, von den Teilnehmenden benötigt werden. Beantwortet man die Frage mit Nein, muss eine Vorgehensweise gewählt werden, bei der zu keinem Zeitpunkt personenbezogene Daten anfallen. Es darf weder nach personenbezogenen Daten gefragt, noch darf aus der Beantwortung anderer Fragen ein Bezug zu einer Person hergestellt werden können. Der Fragebogen muss den potenziellen Teilnehmerinnen und Teilnehmern so zur Verfügung gestellt werden, dass nicht auf Teilnahme oder Nichtteilnahme zurückgeschlossen werden kann. Bei einer solchen einmaligen Befragung müssen auf dem Fragebogen der Zweck der Befragung, die Vorgehensweise und der Verantwortliche benannt werden sowie ein Hinweis auf die Freiwilligkeit der Teilnahme erfolgen. Das unbeobachtete Ausfüllen und die Rückgabe des Fragebogens müssen gewährleistet werden (z. B. ein Briefkasten auf dem Weg zum Ausgang). Bei dieser Vorgehensweise würde der Grundsatz der Datenvermeidung (Vermeidung des Personenbezugs) umgesetzt. Ein Beispiel für eine solche anonyme Befragung ist ein Bewertungsbogen einer Reha-Einrichtung, die Patientinnen und Patienten mit ihren Reha-Unterlagen erhalten.

Werden Personen zu mehreren Zeitpunkten befragt, bspw. zu Beginn, am Ende des Reha-Aufenthaltes und 6 Monate später, so muss die Frage nach der Erfassung von personenbezogenen Daten bejaht werden. Diese werden benötigt, um Teilnehmerinnen und Teilnehmern in der Follow-up-Befragung zu erreichen. Wenn die Wissenschaftlerinnen und Wissenschaftler die Teilnehmenden unmittelbar ansprechen und selbst die Namen und Kontaktdaten erfahren, gelten zu allererst die Datenschutzbestimmungen der Forschungseinrichtung. Ein privates Forschungsinstitut muss das BDSG beachten, eine Universität das einschlägige LDSG, eine Reha-Einrichtung das Sozialgesetzbuch.

Für das Forschungsprojekt ist ein Datenschutzkonzept zu erstellen. Dieses hat Einfluss auf die Gestaltung der Vorgehensweise bei der Datenerhebung und beim weiteren Umgang mit den personenbezogenen Daten. In **Tab. 2** ist zusammengefasst, was für die Erstellung eines Datenschutzkonzeptes zu beachten und festzulegen ist.

Das Datenschutzkonzept muss aus datenschutzrechtlicher Sicht den Lebenszyklus der Forschungsdaten von der Erhebung bis zur Löschung der personenbezogenen Daten regeln. Aus ethischer

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Tab. 2 Aspekte, die bei der Erstellung des Datenschutzkonzeptes Berücksichtigung finden sollten.

Welchem konkreten Zweck (ggf. mehreren Zwecken) dient das Projekt (Zweckbestimmung = Zweckbindung)?
Woher sollen die Forschungsdaten gewonnen werden? Zum Beispiel durch Befragung der Probandinnen und Probanden mittels Fragebogen.
Wozu ist es (zwingend) notwendig, Namen und Kontaktdaten der Teilnehmenden zu erheben? Zum Beispiel, um aus ethischen Gründen den Nachweis führen zu können, dass die Daten auf Basis freiwilliger Einwilligung mitgeteilt oder dass Forschungsdaten rechtmäßig erhoben und nicht fingiert wurden. Ein weiterer Punkt ist es, Namen und Kontaktdaten von Teilnehmenden zu kennen, um sie zu verschiedenen Zeitpunkten zu befragen. Denkbar ist es auch, dass Namen und weitere Angaben benötigt werden, um Daten der Teilnehmenden in verschiedenen Datenquellen aufzufinden und als Forschungsdaten erheben zu können (siehe hierzu den Abschnitt „Verwendung ergänzender Daten aus weiteren Datenquellen“).
Zu klären ist
auf welcher Rechtsgrundlage die personenbezogenen Daten erhoben und für die Forschungszwecke verwendet werden dürfen (siehe auch Datenschutzgrundsätze der Zulässigkeit, der Zweckbestimmung und Zweckbindung, der Datensparsamkeit).
ob Rechtsvorschriften dazu verpflichten, die Forschungsdaten (= Primärdaten) zu anonymisieren oder von den Namen zu trennen (z. B.: § 40 BDSG, § 67c Abs. 5 SGB X). Dann muss festgelegt werden, wie die Datentrennung vorgenommen werden soll und durch wen sie erfolgt.
Wer verwahrt die Einwilligungen?
Wer verwahrt die Zuordnungslisten?
Wie kann das Verwahren so erfolgen, dass Unbefugte keinen Zugriff erhalten?
Wie lange sollen/dürfen die personenbezogenen Daten aufbewahrt werden?
Der Umgang mit den pseudonymen Primärdaten muss geregelt werden (Veränderungsschritte bei der Aufbereitung, Zusammenfügen von Daten aus verschiedenen Quellen, Archivierung).

Sicht muss das Konzept sogar die Zweckbestimmung und Zweckbindung der Primärdaten bis zur abschließenden Löschung der (irgendwann anonymen) Primärdaten gewährleisten (siehe Datenschutzgrundsatz der Zweckbestimmung und Zweckbindung). Die Datenerhebung in Forschungsprojekten kann nur auf Basis von freiwilliger und informierter Einwilligung durchgeführt werden. Je nach Setting, in dem die Datenerhebung stattfindet, müssen zusätzlich die einschlägigen Datenschutzvorschriften beachtet werden, bspw. im Rahmen von Forschung im beruflichen Kontext die jeweiligen Vorschriften zum Arbeitnehmerdatenschutz. Hierüber muss sich die Wissenschaftlerin/der Wissenschaftler im Vorfeld der Datenerhebung informieren.

Teilnehmerinformation und Einwilligungserklärung

Sofern keine andere Rechtsgrundlage gegeben ist, dürfen personenbezogene Daten nur mit Einwilligung erhoben, verarbeitet oder genutzt werden. Die Einwilligung ist durch Gesetze geregelt. „Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben“ (§ 67b Abs. 2 SGB X). Andere Gesetze regeln die Einwilligung inhaltsgleich. Es muss sich stets um eine sog. „informierte Einwilligung“ handeln. Hier besteht eine enge Überschneidung zum „informed consent“ des Weltärztebundes.

Die Einwilligung muss freiwillig, also ohne „faktischen Zwang“ erteilt werden. Der Betroffene muss Handlungsalternativen haben und diese auch erkennen oder verstehen können.

Es empfiehlt sich der folgende Ablauf: Teilnehmerinformation – Bedenkzeit mit Fragemöglichkeit – förmliche Erklärung regelmäßig als schriftliche Einwilligung. Unzulässig wäre im Übrigen eine förmliche Erklärung über die „Nicht-Teilnahme“ oder die Erklärung, dass keine personenbezogenen Daten verwendet werden dürfen. Das würde personenbezogene Daten hinterlassen, was der Betroffene ja gerade nicht will.

In der Teilnehmerinformation sollten die folgenden Punkte enthalten sein [3]:

- Titel bzw. Name des Forschungsprojektes;
- verantwortliche Institution/Personen für das Vorhaben und Ansprechpartner;
- Beschreibung der Zweckbestimmung des Vorhabens (mit inhaltlichem Bezug zur Datenquelle oder Institution, bei der Forschungsdaten erhoben werden sollen). Hier reicht es nicht aus, zu schreiben „die Daten werden genutzt für wissenschaftliche Zwecke“. Es muss eine hinreichende Beschreibung der Zweckbestimmung erfolgen;
- Beschreibung des Ablaufs der Datenerhebung (Art und Umfang der Daten mit inhaltlichem Bezug zu Datenquellen oder Institutionen, bei denen Forschungsdaten erhoben werden sollen);
- Hinweise zum Datenschutz (z. B. Erklärung der Pseudonymisierung oder Anonymisierung und Löschung der Daten). Der Hinweis, dass die Datenschutzgesetze eingehalten werden, reicht nicht aus!;
- Hinweise zur Freiwilligkeit der Teilnahme. Hierzu gehören u. a. Hinweise, dass nichts zu tun ist, wenn man nicht teilnehmen möchte sowie Erläuterungen, dass keine Nachteile aus einer Nichtteilnahme entstehen, oder die Widerrufsmöglichkeit der Einwilligung;
- Bitte um Teilnahme.

Ein Muster dazu hat die Deutsche Rentenversicherung Bund auf ihrer Website zum Download bereitgestellt [3].

Folgende Punkte müssen in einer Einwilligungserklärung stehen, um den Datenschutz zu gewährleisten [4]:

Dem Teilnehmer wird versichert, dass

- die Teilnahme freiwillig ist;
- die Teilnahme jederzeit ohne Nachteile widerrufen werden kann;
- keine personenbezogenen Angaben (Name, Geburtsdatum, Adresse) oder sonstige Angaben, die Rückschlüsse auf die Person zulassen, an Dritte weitergegeben werden. Hinweis: Falls Ergebnisdaten oder andere erhobene Daten mit Personenbezug veröffentlicht werden sollen, dann muss das wahrheitsgemäß erwähnt werden. Nur mit einer Einwilligung der Betroffenen ist eine solche Veröffentlichung zulässig. Im Falle von Fotos mit erkennbaren Personen muss die Einwilligung vorliegen, auch wenn kein Name genannt wird (Recht am eigenen Bild);

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

- die Angaben anonym (oder personenbezogen) verwendet werden;
- alle im Zusammenhang mit der Untersuchung erhobenen Daten gelöscht werden, sobald sie für die weitere wissenschaftliche Auswertung nicht mehr erforderlich sind (s. Archivierung der Daten).

Auch hier hält die Deutsche Rentenversicherung Bund ein Muster vor [4].

Abschließend kann empfohlen werden, dass die Teilnehmerinformation immer beim Betroffenen verbleiben sollte, damit er sie jederzeit nachlesen kann. Den Teilnehmenden sollten 2 Exemplare der Einwilligungserklärung ausgehändigt werden. Ein Exemplar wird unterschrieben an die Wissenschaftlerin/den Wissenschaftler zurückgegeben und das zweite behält die Studienteilnehmerin/der Studienteilnehmer für die persönlichen Unterlagen.

Für die informierte Zustimmung muss die erforderliche Einsichtsfähigkeit vorhanden sein. Bei Studien mit dementen oder psychisch erkrankten Patienten könnten informierte Einwilligungen in Frage kommen, die stellvertretend für die Patienten durch Angehörige oder ihren gesetzlichen Betreuer getätigt werden; allerdings gibt es dazu keine klaren gesetzlichen Bestimmungen [5]. Bei Befragungen von Minderjährigen muss über deren Einsichtsfähigkeit eine Annahme getroffen werden: Kann ein Minderjähriger die Konsequenzen der Verwendung seiner Daten übersehen, dann kann er über eine Teilnahme entscheiden, sonst ist die Einwilligung des gesetzlichen Vertreters einzuholen. Eine klare Altersgrenze gibt es hier nicht, vielmehr ist es jeweils eine Einzelfallentscheidung. Bei Minderjährigen unter 14 Jahren ist jedoch grundsätzlich davon auszugehen, dass sie die Folgen einer Einwilligung nicht überblicken können und somit eine Einwilligung der gesetzlichen Vertreter notwendig ist [2]. Im Lebensabschnitt von 14 bis 18 Jahren ist dennoch sinnvoll, den betroffenen Minderjährigen und die Erziehungsberechtigten zu informieren und von beiden den „informed consent“ einzuholen.

Die schriftliche Einwilligungserklärung muss aufbewahrt werden, solange personenbezogene Forschungsdaten vorhanden sind. Die Einwilligungserklärung wird nicht mehr benötigt, wenn die Forschungsdaten anonymisiert werden. Dann muss diese sie vernichtet werden (§ 84 SGB X, § 35 BDSG).

Verwendung ergänzender Daten aus weiteren Datenquellen

Ergänzend zu den Primärdaten können weitere Daten aus anderen Datenquellen, wie z. B. aus dem Reha-Entlassungsbericht oder mittels eines Kurzfragebogens, ausgefüllt durch den behandelnden Arzt, hinzugefügt werden, um bspw. die genaue Diagnose für die Auswertung zu nutzen. Dazu ist es notwendig, diese weiteren Zweckbestimmungen im Datenschutzkonzept ausdrücklich zu benennen und zu begründen (siehe Ausführungen zu Datensparsamkeit, Angemessenheit, Geeignetheit). In der Teilnehmerinformation muss ausdrücklich erwähnt werden, bei welchen Stellen die ergänzenden Daten erhoben werden sollen, warum und um welche Daten es sich handelt. Für jede Stelle (Datenquelle) muss eine inhaltlich hinreichend bestimmte Einwilligung für konkret zu übermittelnde Daten vorhanden sein.

Nutzung von Sozialdaten in der Rehabilitationsforschung

Sozialdaten sind personenbezogene Daten und Daten juristischer Personen, die bei Sozialleistungsträgern für deren Aufgabenerfüllung nach dem Sozialgesetzbuch anfallen. Im Allgemeinen werden Sozialdaten nicht für Forschungszwecke erhoben. Eine Nutzung für die Forschung stellt eine Zweckänderung dar. Die vorhandenen Sozialdaten bei den Sozialleistungsträgern oder in den Reha-Einrichtungen dürfen für Forschungszwecke nur verwendet werden, wenn eine Rechtsvorschrift aus dem SGB dies ausdrücklich zulässt (Zulässigkeitsgrundsatz).

Die Sozialleistungsträger dürfen die vorhandenen Sozialdaten für eigene Vorhaben der wissenschaftlichen Forschung oder für Planungsvorhaben im Sozialleistungsbereich nutzen (§ 67c Abs. 2 Nr. 3 SGB X in Verbindung mit § 75 Abs. 1 SGB X). Andere Stellen können die Sozialleistungsträger um die Übermittlung von vorhandenen Sozialdaten für Forschungszwecke bitten. Die Übermittlung an andere Stellen ist in § 75 SGB X geregelt. Aus Gründen der Gleichbehandlung bei der Zweckänderung der Sozialdaten für die Forschung gelten für die Sozialleistungsträger und für externe Wissenschaftlerinnen und Wissenschaftler dieselben Voraussetzungen für die Verwendung der Sozialdaten für Forschungszwecke. „Forschung“ in dieser Vorschrift bedeutet, dass nur Forschungsprojekte im Sozialleistungsbereich in Betracht kommen. Forschungsprojekte über historische Persönlichkeiten oder historische Forschung oder Markt- und Meinungsforschung scheiden damit aus. Zudem muss es sich um ein „bestimmtes“ Vorhaben handeln, das Thema klar abgegrenzt und der Datenkatalog festgelegt sein. Die Bestimmtheit verbietet die Verwendung der anfallenden Sozialdaten für andere Projekte oder für vergleichende Auswertungen.

Voraussetzung für viele Forschungsvorhaben ist, dass die Forschungsdaten Personen zuordenbar sein müssen. Der Sozialleistungsträger oder die externen Wissenschaftlerinnen und Wissenschaftler müssen also Forschungsdaten mit Personenbezug erhalten oder die Zuordnung zum Namen wieder herstellen können. So lange die Identifizierung einzelner Personen möglich bleibt, wird von Sozialdaten gesprochen.

Kann das Forschungsziel auf andere Weise, nämlich durch Nutzung anonymer Daten erreicht werden, ist eine Übermittlung der Forschungsdaten ohne Personenbezug aus datenschutzrechtlicher Sicht immer zulässig (§ 75 Abs. 1 Satz 2 SGB X). Sobald der Personenbezug unwiederbringlich gelöscht ist, liegen keine Sozialdaten mehr vor (Anonymisierung). Zugleich ist bei einem solchen Vorgehen der beschriebene Grundsatz der Datenvermeidung erfüllt.

Bleibt jedoch der Personenbezug erhalten, darf die Nutzung oder Übermittlung der Sozialdaten nicht gegen schutzwürdige Interessen der Betroffenen verstoßen. Dies kann immer nur im Einzelfall geprüft werden. Am besten, der Betroffene wird zuvor informiert und um Einwilligung gebeten. Genau dieser Weg wird in Satz 2 der Vorschrift auch verlangt, zumindest wenn es zumutbar ist. Liegt die Einwilligung vor, darf ausgewertet werden, was durch die Einwilligung abgedeckt wird.

In Projekten, in denen das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt, dürfen Sozialdaten unter Beibehaltung des Personenbezugs grundsätzlich auch ohne Einwilligung genutzt oder übermittelt werden. Die Übermittlung bedarf der vorherigen Genehmigung durch die oberste Bundes- oder Landesbehörde, die für den Sozialleistungsträger, aus dem die Daten herrühren, zuständig ist

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

(§ 75 Abs. 2 SGB X). Die Wissenschaftlerinnen und Wissenschaftler müssen diese Genehmigung einholen und dabei nachweisen, warum das öffentliche Forschungsinteresse an dem eigenen Projekt das Geheimhaltungsinteresse der Betroffenen überwiegt. Es muss also ausreichend begründet werden, warum personenbezogene Daten auch ohne „Wissen und Wollen" der Betroffenen zur Erreichung des Forschungsziels erforderlich sind. Die Praxis zeigt aber, dass die Ziele der meisten Projekte mit anonymen Daten oder mit der Einwilligung der Betroffenen erreicht werden können, sodass diese Regelung in den wenigsten Fällen zur Anwendung kommt. Bei jeder Datenübermittlung ist § 78 SGB X zu beachten. Die Wissenschaftlerinnen und Wissenschaftler dürfen die empfangenen personenbezogenen Forschungsdaten nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind. Eine personenbezogene Nutzung dieser Sozialdaten für andere Forschungsprojekte ist deshalb unzulässig. Zudem müssen die Wissenschaftlerinnen und Wissenschaftler die Daten in demselben Umfang geheim halten wie die Sozialleistungsträger.

Einbeziehung von Datenschutzbeauftragten und Ethikkommission

▼

Bereits bei der Entwicklung der Abläufe sollte eine Datenschutzbeauftragte/ein Datenschutzbeauftragter zur Einhaltung des Datenschutzes mit einbezogen werden. Eine Stellungnahme eines Datenschützers zu seinem eigenen Datenschutzkonzept einzuholen, ist nicht verpflichtend, da es dazu keine Vorschriften oder Gesetze gibt. Dies ist eine Empfehlung an die Wissenschaftlerin/den Wissenschaftler, um sich selbst im Rahmen des Forschungsvorhabens abzusichern. Allerdings kann der Geldgeber fordern, eine Stellungnahme einzuholen. Falls Daten aus Datenquellen anderer Stellen erhoben werden sollen, kann auch der Datenschutzbeauftragte dieser Stelle einbezogen werden, insbesondere zur Abstimmung der Teilnehmerinformation und Einwilligungserklärung. Bei Forschungsvorhaben, die in verschiedenen Regionen durchgeführt werden, können sich die zuständigen Datenschützer untereinander abstimmen, aber auch das ist kein Muss.

Das Votum einer Ethikkommission muss eingeholt werden, wenn es sich um medizinische Forschungsvorhaben handelt, die unter folgende Regelungen fallen: Arzneimittelgesetz, Medizinproduktegesetz, Röntgen- und Strahlenschutzverordnung oder Transfusionsgesetz. Ist der Forscher – gemäß der Berufsordnung – einer Ärztekammer angehörig, muss ebenfalls ein Votum eingeholt werden. In der psychologischen und epidemiologischen Forschung mit personenbezogenen Daten ist die Einholung eines Ethikvotums gebräuchlich. Alle Forschungsvorhaben, die nicht unter spezielle Regelungen fallen, können dies freiwillig tun. Da mittlerweile viele wissenschaftliche Fachzeitschriften das Votum einer Ethikkommission für die Veröffentlichung von Forschungsdaten fordern, ist es empfehlenswert, ein solches zu beantragen. Hierbei ist es sinnvoll, neben den Unterlagen zur Studie auch die Stellungnahme des Datenschutzbeauftragten vorzulegen [5]. Falls das Forschungsvorhaben in mehreren Regionen durchgeführt wird, gibt es eine federführende Ethikkommission, die für den Standort des Projektleiters zuständig ist. Dieses ist die hauptverantwortliche Kommission. Die Ethikkommissionen der anderen Regionen sind beteiligte Kommissionen. Diese bewerten die Qualifikationen der Prüfer und die Geeignetheit der federführenden Ethikkommission und geben dieser jeweils eine Rückmeldung ihrer Bewertung [6].

Umgang mit Forschungsdaten und deren Veröffentlichung

▼

Nach der Erhebung von Forschungsdaten spricht man zunächst von Primärdaten. Je nach Gestaltung des Projektes können dies anonyme, pseudonyme oder personenbezogene Daten sein. Bei eigens erhobenen Daten mit Personenbezug schreiben die Datenschutzgesetze vor, Studiendaten möglichst bald zu pseudonymisieren oder zu anonymisieren (→ Glossar) (§ 40 Abs. 2 BDSG, § 67c Abs. 5 SGB X). Eine erneute Verknüpfung mit den Namen ist nur zulässig, wenn dies erforderlich ist. Es sollte Festlegungen geben, wann und zu welchen Zwecken die Primärdaten den Namen wieder zugeordnet werden dürfen.

Wichtig ist dabei, zwischen einer Pseudonymisierung und der Anonymisierung zu unterscheiden (§ 3 Abs. 6 und Abs. 6a BDSG). Werden Daten derselben Person aus verschiedenen Quellen erhoben oder ist eine mehrmalige Befragung des Studienteilnehmers geplant, dann empfiehlt sich eine Pseudonymisierung (die Ersetzung des Namens durch einen Code). Sollen bspw. Sozialdaten mit Befragungsdaten verknüpft werden, so muss dem Halter der Sozialdaten der Name und das Pseudonym genannt werden. Die Sozialdaten werden vom Datenhalter mit dem Pseudonym gekennzeichnet und nur mit Pseudonym an den Forschenden übermittelt. Die Zuordnungsliste der Namen zu den Pseudonymen muss getrennt von den Forschungsdaten und vor Unbefugten geschützt aufbewahrt werden. Dies kann z. B. bei einem Datentreuhänder erfolgen. Anhand des Pseudonyms können Daten aus verschiedenen Quellen für die Auswertung verknüpft werden.

Sollen die Daten anonymisiert werden, ist darauf zu achten, dass tatsächlich keine Person identifizierbar ist. Wenn Daten einer oder weniger Personen mit seltenen Erkrankungen in Kombination mit weiteren Variablen dargestellt werden und die Fallzahl auf 5 oder weniger sinkt, können Personen mit zunehmender Wahrscheinlichkeit identifiziert werden. In datenschutzrechtlicher Diskussion stehen dabei auch personbezogene Faktoren der Klassifikation der Funktionsfähigkeit, Behinderung und Gesundheit (ICF) [7]. In solchen Fällen sollten die Zellbesetzungen nicht veröffentlicht werden oder versucht werden, durch Kombination von 2 Ausprägungen einer Variablen die Fallzahl zu vergrößern.

Folgende Schritte sollten bis zur Anonymität durchgeführt werden:

- Erhebung der Forschungsdaten aus personenbezogenen Datenquellen;
- Aufzeichnen der Forschungsdaten ohne Personenbezug (pseudonyme Primärdaten, Datentrennung nach § 40 BDSG);
- Löschen der Pseudonyme und Zuordnungslisten vor der Auswertung (anonymisieren);
- Auswertung und Ergebnisdarstellung mit mindestens faktisch anonymen Daten.

Die Verantwortung dafür liegt bei den Forschenden.

Am Ende aller Datenerhebungen sind Namen und Kontaktdaten aus datenschutzrechtlicher Sicht nicht mehr erforderlich und müssen gelöscht werden, wenn nicht durch Gesetz oder andere zwingende Regelungen eine Aufbewahrungs- oder Archivierungspflicht besteht, z. B. durch den Geldgeber/Förderer. Die

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Wissenschaftlerinnen und Wissenschaftler müssen dann jedoch gewährleisten, dass die Löschung der personenbezogenen Daten nach Ablauf der Archivierungspflicht tatsächlich erfolgt. Bei der Löschung müssen auch die Einwilligungen und Namenslisten gelöscht werden, die ebenfalls einen Personenbezug haben. Alle Auswertungen und Ergebnisdarstellungen sollten anonym erfolgen, selbst wenn die Primärdaten während der Archivierungspflicht noch den Namen zugeordnet werden könnten. Die Daten müssen für den gesamten Zeitraum vor Missbrauch geschützt werden (Zugriff durch Fremde, Nutzung für andere Projekte usw.). Das stellt einen erheblichen Aufwand dar und kann über längere Zeiträume betrachtet auch kostenintensiv sein. Neben datenschutzrechtlichen Forderungen sprechen also auch eigene Interessen der Wissenschaftlerinnen und Wissenschaftler an einer „schlanken und kostengünstigen Verwaltung" für die frühzeitige Anonymisierung der Forschungsdaten.

Rechtsfolgen bei Verstößen

Wird den Regelungen zum Datenschutz in der Forschung nicht entsprochen, kann es in der Folge zu Schadensersatzforderungen (§ 7ff BDSG), einer Geldstrafe oder zu einem Freiheitsentzug von bis zu 2 Jahre kommen. Dieses ist in § 44 BDSG (Strafvorschriften) und in § 85a SGB X (Strafvorschriften) festgelegt.
Für öffentliche Stellen gilt gemäß § 8 BDSG das Prinzip der Gefährdungshaftung bei automatisierter Datenverarbeitung, d. h., die Schadensersatzpflicht besteht unabhängig von einem Verschulden. § 8 Abs. 2 BDSG formuliert den Anspruch auf Schmerzensgeld bei einer schweren Verletzung des Persönlichkeitsrechts. Der Image-Schaden für die betroffenen Wissenschaftlerin/den Wissenschaftler ist ebenfalls zu bedenken.

Archivierung der Daten

Eine Empfehlung zur „Sicherung guter wissenschaftlicher Praxis" der Deutschen Forschungsgemeinschaft (DFG) lautet, dass Primärdaten für 10 Jahre „auf haltbaren und gesicherten Trägern" [8] aufbewahrt werden sollen, um jeden Vorgehensschritt zwecks Überprüfung transparent zu halten [8]. Eine generelle gesetzliche Pflicht zur Archivierung wissenschaftlicher Primärdaten besteht jedoch nicht. Aus datenschutzrechtlicher Sicht kann diese Ordnungsmäßigkeit ohne die vollständige Aufbewahrung aller personenbezogenen Daten gewährleistet werden. Zum Beispiel könnten bestimmte Arbeitsschritte von unabhängiger Stelle revisionssicher (→ Glossar) geprüft und dokumentiert werden. Denkbar wäre auch, bestimmte Arbeitsschritte mit personenbezogenen Daten über einen Datentreuhänder abwickeln zu lassen, wie in dem Beispiel aus der Praxis in diesem Beitrag.
Maßgeblich für den Aufbewahrungszeitraum sollte dabei nicht das Alter der Daten selbst sein, sondern – auch im Sinne der Nachnutzbarkeit – das Datum einer Veröffentlichung, die auf diesen Daten beruht [9]. Der Zeitraum der Archivierung kann sich also erheblich verlängern, wenn bspw. erhobene Daten für mehrere Publikationen verwendet werden.
Bei Verfügbarkeit von Primärdaten in Papierform ist die Archivierungspflicht als erfüllt anzusehen. Interessanter jedoch und in zunehmendem Maße wichtig ist die Archivierung digital verfügbarer Primärdaten. Die Empfehlungen zur Aufbewahrung und Bereitstellung wissenschaftlicher Primärdaten der DFG definieren einen Rahmen, der für die Datenarchivierung festlegt, welche Daten archiviert werden, welches Organisationskonzept anzuwenden ist, welche Standards einzuhalten sowie welche Metadaten anzuwenden sind [10]. Insbesondere wird auch die freie Zugänglichkeit von Daten geregelt, jedoch bleiben die Belange schützenswerter, personenbezogener Daten unberücksichtigt. Grundsätze zum Umgang mit Forschungsdaten definiert auch die Allianz der deutschen Wissenschaftsorganisationen [11], die diesen Aspekt zumindest in allgemeiner Form erwähnt: „Dabei sind die wissenschaftlichen und rechtlichen Interessen der Forscherinnen und Forscher, der Schutz persönlicher Daten von Probanden, Patienten und anderen von den erhobenen Daten betroffenen Personen sowie weitere Verpflichtungen gegenüber Dritten – etwa Kooperationspartnern – zu beachten". Insbesondere der Schutzaspekt persönlicher Daten steht dabei im direkten Konflikt zur Forderung der DFG nach freiem Zugang zu den Daten. Daher sind geeignete Archivierungsformen zu wählen, die beiden Anforderungen gerecht werden. Die Situation verkompliziert sich weiter, wenn ein Geldgeber für ein Forschungsvorhaben weitere Anforderungen stellt – im Zweifelsfall muss zwischen Wissenschaftlern, Geldgebern und Datenschützern eine jeweils passende Lösung vereinbart werden [12], die natürlich die rechtlichen Rahmenbedingungen einhält. Dem Aspekt der Aufbewahrung und ggf. des „freien Zugangs zu personenbeziehbaren Primärdaten" kommt deshalb bei der Planung und Gestaltung des Forschungsprojektes von Anfang an eine wesentliche Bedeutung zu. Falls die Forschenden die Absicht verfolgen, die Primärdaten mit Personenbezug der Fachöffentlichkeit relativ frei oder sogar jedermann über das Internet zugänglich zu machen, dann ist das datenschutzrechtlich nicht verboten. Von jedem Beteiligten muss dann die Einwilligung vorliegen, mit dieser Art der Veröffentlichung einverstanden zu sein.
Werden personenbezogene Daten automatisiert verarbeitet, müssen insbesondere Maßnahmen zur Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sowie zum Trennungsgebot unternommen werden (Anlage zu § 9 BDSG bzw. zu § 78a SGB X – „8-Punkte-Katalog"). Automatisiert ist die Verarbeitung, wenn Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch Verwendung von Computern geschieht.
Das Wort „insbesondere" deutet an, dass es sich nicht um eine abschließende Aufzählung handelt, sondern dass die konkreten Maßnahmen immer vom Schutzbedarf der Daten abhängig sind. Die Anlage zu § 9 BDSG oder zu § 78a SGB X bestimmt seit ihrer Anpassung im Jahr 2010, dass als Maßnahmen für die Zugangs-, Zugriffs- und Weitergabekontrolle dem Stand der Technik entsprechende Verschlüsselungsmethoden eingesetzt werden sollten.
Wesentlich sind folgende Punkte:

- Das Trennungsgebot: Daten, die für einen bestimmten (Forschungs-)Zweck erhoben wurden, müssen getrennt von Daten anderer (Forschungs-)Zwecke verarbeitet werden. Die Trennung von verschiedenen Projekten muss nicht vollständig physikalisch (auf getrennten Computern) erfolgen, sondern kann auch als „logische Trennung" in Verbindung mit den folgenden Kontrollpunkten erreicht werden.
- Zugangs-, Zugriffs- und Eingabekontrolle: Insbesondere durch eine Benutzerverwaltung kombiniert mit einem Rechte- und Rollenkonzept muss gesteuert werden, welche Personen die Computer und die Programme in Betrieb nehmen dürfen. Jedem Nutzer muss eine der Aufgabe entsprechende Zugriffsrolle zugeordnet werden, die festlegt, auf welche Datensätze

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

oder Teildatensätze lesend/schreibend zugegriffen werden darf. Die Nr. 3 der Anlage zu § 9 BDSG oder zu § 78a SGB X verlangt auch die Protokollierung der Zugriffe. Nachvollziehbar muss sein, wer wann auf welche Daten zugegriffen hat und welche Veränderungen gegebenenfalls vorgenommen wurden. Die Nr. 5 der Anlage zu § 9 BDSG oder zu § 78a SGB X verlangt auch, dass erkennbar sein muss, wer die Eingaben getätigt hat (Eingabekontrolle).

- Weitergabekontrolle: Bei automatisierter Weitergabe personenbezogener Forschungsdaten an andere Stellen oder Personen muss insbesondere gewährleistet werden, dass während der Übertragung keine unbefugte Kenntnisnahme oder Veränderung erfolgt. Hier ist eine Verschlüsselung das Mittel der Wahl. Auch das ist keine triviale Aufgabe, da Sender und Empfänger dieselbe Technologie verwenden müssen und der Schlüssel zum Ver- oder Entschlüsseln auf einem „sicheren Weg“ ausgetauscht werden muss.
- Verfügbarkeitskontrolle: Daten müssen verfügbar sein und vor zufälliger oder mutwilliger Beschädigung und Zerstörung geschützt werden. Üblich sind regelmäßige Sicherheitskopien, die auch gegen unbefugte Kenntnisnahme geschützt werden sollten (Verschlüsselung). Bei der Löschung von Daten muss auch gewährleistet werden, dass die Sicherheitskopien gelöscht werden. Bei der Aussonderung „alter Festplatten“ oder Austausch bei Defekt muss an eine mechanische oder magnetische Zerstörung gedacht werden.

Primärdaten sollten deshalb stets pseudonym gespeichert werden, also ohne die Namen der Betroffenen. Die Zuordnungsliste sollte getrennt und am besten auf einem anderen Medium, also Papier oder einem getrennt gespeicherten Datenträger mit restriktiven Zugriffsrechten aufbewahrt werden. Die Primärdaten gelten datenschutzrechtlich zwar immer noch als personenbeziehbar und die obigen Kontrollgebote müssen umgesetzt werden. Allerdings würde ein Verlust oder eine beiläufige Kenntnisnahme durch Unbefugte nicht dazu führen, dass personenbezogene Daten bekannt werden.

Forschungsdaten und personenbezogene Daten müssen auch während der Archivierung getrennt voneinander gespeichert werden, um eine Rückverfolgbarkeit zu Individuen zu erschweren (§ 40 BDSG). Sensible Daten dürfen nicht auf einem mobilen Rechner gespeichert und auch nicht ohne geeigneten Schutz (Verschlüsselung und Signatur [→ Glossar]) per E-Mail versendet werden (siehe Punkt „Weitergabekontrolle“).

Um geeignete Archivierungsformen entwickeln bzw. auswählen zu können, definiert das Open Archive Information Systems Referenzmodell (OAIS) einen Rahmen, bestehend aus den Aufgabenbereichen Datenübernahme, Datenaufbewahrung, Datenmanagement, Systemverwaltung, Planung der Langzeitarchivierung und Zugriff [13]. In Anlehnung an das OAIS hat die Physikalisch-Technische Bundesanstalt (PTB) das ArchiSave Schutzprofil entwickelt [14], das einen Katalog an Sicherheitsanforderungen für die Entwicklung digitaler Langzeitarchive definiert. Durch den kontrollierten Einsatz von Archivsystemen gemäß OAIS/ArchiSafe ist den Anforderungen an die Archivierung Genüge getan. Alternativ zu einem komplexen Archivsystem kann ein Datenschutzrechner eingesetzt werden. Mit sicherem Passwort geschützte, eingeschränkt zugängliche Datenschutzrechner ohne Netzanschluss speichern Daten und stellen sie auswertbar zur Verfügung. Die Anforderungen an ein sicheres Passwort sollten dazu möglichst in einer Passwortrichtlinie festgelegt sein, die regelmäßig weiterentwickelt wird. Auf dem Datenschutzrechner können Daten zusätzlich verschlüsselt und elektronisch signiert werden [15]. Wichtig ist, dass Archivierungsverfahren regelmäßig aktualisiert werden müssen, um mit dem technischen Wandel in Sicherheitsverfahren, Datenformaten und verwendeten Datenträgern Schritt zu halten [16]. Für die zu archivierenden Daten bedeutet dies, dass die technischen Anforderungen an Datenformate so gering wie möglich ausfallen sollten. Ideal ist die Verwendung einfachster Textformate und weitverbreiteter Medienformate für Bild-, Video-, Audiodaten. Insgesamt ist die Langzeitarchivierung (insbesondere komplexerer Datenformate) ein noch nicht standardisiert lösbares Problem, das im Einzelfall betrachtet werden muss und das Gegenstand aktueller Forschungsvorhaben ist [17].

Fazit

Wenn bei einem Forschungsprojekt auf personenbezogene Daten zugegriffen werden soll oder die Wissenschaftlerinnen und Wissenschaftler mit personenbezogenen Daten umgehen, ist die Beachtung des Datenschutzes eine Rechtspflicht. Daher muss für die Wissenschaftlerin/den Wissenschaftler der vertrauliche Umgang mit personenbezogenen Daten eine Selbstverständlichkeit sein. Den potenziellen Studienteilnehmerinnen und -teilnehmern muss das Projekt und insbesondere der Umgang mit „ihren Daten“ transparent und verständlich beschrieben werden (Teilnehmerinformation). Forschungsdaten mit Personenbezug dürfen regelmäßig erhoben werden, wenn eine informierte Einwilligung des Betroffenen vorliegt. Diese muss freiwillig, also ohne Druck oder Zwang abgegeben worden sein. Diese Vorgehensweisen entsprechen den Gesetzen und stehen im Einklang mit den Persönlichkeitsrechten der Betroffenen und den Ethikgrundsätzen des Weltärztebundes (informed consent). Die Praxis zeigt auch, dass es regelmäßig gelingt, Sozialdaten für die Forschung zu verwenden, dabei aber bereits vor der Datenübermittlung die Namen durch Pseudonyme zu ersetzen oder die Daten völlig zu anonymisieren. Gelingt es, Sozialdaten bei der Datenquelle völlig zu anonymisieren, dürfen diese ohne Zustimmung des Betroffenen ausgewertet werden. Bei einem Forschungsvorhaben ist zu empfehlen, sowohl zur Absicherung der Wissenschaftlerin/des Wissenschaftlers als auch der Studienteilnehmerin/des -teilnehmers, die Vorgehensweise von einem Datenschützer prüfen zu lassen. Dazu zählt die Aufklärung und Information der zu Befragenden, der Umgang mit den Forschungsdaten wie Datenhaltung, Auswertung und Veröffentlichung. Bei der digitalen Datenhaltung ist zu empfehlen, einen IT-Fachmann oder Dokumentar hinzuziehen, um die Daten sicher zu speichern und zu archivieren.

Kernbotschaft

Datenschutz in der rehabilitativen Forschung muss im Interesse der Forschenden als auch der Studienteilnehmenden eingehalten werden. Nur bei der Berücksichtigung aller datenschutzrelevanten Aspekte in einem Forschungsprojekt kann von einem vertraulichen Umgang mit personenbezogenen Daten und der Wahrung der Persönlichkeitsrechte gesprochen werden.

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.

Danksagung

Wir danken der Datenschutzbeauftragten der Universität Bielefeld, Ines Meyer, für die inhaltliche Unterstützung und die kritische Durchsicht des Textes.

Interessenkonflikt: Die Autoren geben an, dass kein Interessenkonflikt besteht.

Ergänzendes Material

Das Beispiel aus der Rehabilitationspraxis mit externem Datentreuhänder und dem Ablaufschema Abb. 1 sowie das Glossar zu diesem Beitrag finden Sie online unter www.thieme-connect.de/ejournals/toc/rehabilitation.

Institute

[1] Fakultät für Gesundheitswissenschaften, AG3 – Epidemiologie & International Public Health, Universität Bielefeld
[2] Deutsche Rentenversicherung Bund, Referat für Datenschutz, Berlin
[3] Institut für Rehabilitationsforschung Norderney, Abteilung Sozialmedizin – Deutsche Rentenversicherung Westfalen, Münster
[4] Centre for Learning Science and Technology, Open Universiteit Nederland, Heerlen, Niederlande
[5] Unit for Health Promotion Research, University of Southern Denmark, Esbjerg, Dänemark

Literatur

1 *Weltärztebund (WMA)*. Weltärztebund – Deklaration von Helsinki. Ethische Grundsätze für die medizinische Forschung am Menschen. 18. WMA-Generalversammlung im Juni 1964 in Helsinki. Version 2008, verfügbar unter www.uibk.ac.at/rtf/medizinrecht/helsinki_dek.pdf
2 *Metschke R*, *Wellbrock R*. Datenschutz in Wissenschaft und Forschung. 3., überarb. Aufl. Berlin: Berliner Beauftragter für Datenschutz und Informationsfreiheit; 2002; verfügbar unter www.datenschutz-berlin.de/attachments/47/Materialien28.pdf (aufgerufen 22.12.2011)
3 *Deutsche Rentenversicherung Bund – Referat für Datenschutz*. Anregungen zur Gestaltung einer schriftlichen Teilnehmerinformation. Berlin: DRV Bund; 2011; verfügbar unter www.deutsche-rentenversicherung.de/cae/servlet/contentblob/208220/publicationFile/37621/Datenschutz_Textbausteine_Teilnehmerinformation.pdf (aufgerufen 17.10.2012)
4 *Deutsche Rentenversicherung Bund – Referat für Datenschutz*. Anregungen zur Gestaltung einer schriftlichen Einwilligungserklärung. Berlin: DRV Bund; 2011; verfügbar unter www.deutsche-rentenversicherung.de/cae/servlet/contentblob/208216/publicationFile/37622/Datenschutz_Textbausteine_Einwilligungserklaerung.pdf (aufgerufen 17.10.2012)
5 *Bake C*, *Blobe B*, *Münch P*, Hrsg. Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen. Spezielle Probleme des Datenschutzes und der Datensicherheit im Bereich des Gesundheits- und Sozialwesens (GSW) in Deutschland. 3. Aufl. Frechen: Datakontext; 2009
6 *Bundestag*. Gesetz über den Verkehr mit Arzneimitteln. Zwölftes Gesetz zur Änderung des Arzneimittelgesetzes. Bundesgesetzblatt 2004 Nr. 41
7 *Arbeitsgruppe ICF der Deutschen Gesellschaft für Rehabilitationswissenschaften (DGRW)*. Stellungnahme der DGRW zu „Personbezogene Faktoren der ICF – Entwurf der AG ‚ICF' des Fachbereichs II der Deutschen Gesellschaft für Sozialmedizin und Prävention (DGSMP)". Rehabilitation 2012; 51: 129–130
8 *Deutsche Forschungsgemeinschaft*. Vorschläge zur Sicherung guter Wissenschaftlicher Praxis. Empfehlungen der Kommission „Selbstkontrolle in der Wissenschaft". Weinheim: Wiley-VCH; 1998
9 *Rümpel S*. Der Lebenszyklus von Forschungsdaten. In: *Büttner S*, *Hobohm H*, *Müller L*, Hrsg. Handbuch Forschungsdatenmanagement. Bad Honnef: BOCK+HERCHEN; 2011; 25–34
10 *Deutsche Forschungsgemeinschaft*. Empfehlungen zur gesicherten Aufbewahrung und Bereitstellung digitaler Forschungsprimärdaten. Bonn: Deutsche Forschungsgemeinschaft; 2009; verfügbar unter www.dfg.de/download/pdf/foerderung/programme/lis/ua_inf_empfehlungen_200901.pdf (aufgerufen 16.8.2012)
11 *Allianz der deutschen Wissenschaftsorganisationen*. Grundsätze zum Umgang mit Forschungsdaten. 2010; verfügbar unter www.wissenschaftsrat.de/download/archiv/Allianz_Grundsaetze_Forschungsdaten.pdf (aufgerufen 16.8.2012)
12 *Dragano N*. Datenmanagement: Datentypen, Patiententagebücher, Fragebögen, Korrespondenz, Queries, Ablage von Studienmaterialien, Archivierung. Düsseldorf: Heinrich-Heine-Universität; 2005; verfügbar unter www.refonet.de/veranstaltungen/documents/dragano20051020.pdf (aufgerufen 16.8.2012)
13 *Neuroth H*, *Oßwald A*, *Scheffel R et al.*, Hrsg. nestor Handbuch – Eine kleine Enzyklopädie der digitalen Langzeitarchivierung. Boizenburg: Hülsbusch; 2009; verfügbar unter nestor.sub.uni-goettingen.de/handbuch/artikel/nestor_handbuch_artikel_384.pdf (aufgerufen 17.10.2012)
14 *Zimmer W*. Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents. Bonn: Bundesamt für Sicherheit in der Informationstechnik; 2008; verfügbar unter www.archisafe.de/s/c/EgJsjQEJ/ArchiSafe_Dokumente/ArchiSafe_PP_V10.pdf;jsessionid=407C28FEEDABB09E4EEB5157796EA232 (aufgerufen 17.10.2012)
15 *McDowell M*, *Rafail J*, *Hernan S*. Security Tip (ST04-002). Choosing and Protecting Passwords. 2009; verfügbar unter www.us-cert.gov/cas/tips/ST04-002.html (aufgerufen 17.10.2012)
16 *Schmücker P*. Elektronische Archivierung im Krankenhaus: Wo stehen wir heute? 30. Deutscher Krankenhaustag, Tag der Informationstechnologie, Fachforum „IT im Krankenhaus: Gesundheitskarte, Archivierung, Netze". Mannheim: Hochschule Mannheim; 2007; verfügbar unter www.deutscher-krankenhaustag.de/de/vortraege/pdf/07.Schmuecker.pdf (aufgerufen 16.8.2012)
17 *Dickmann F*. LABIMI/F – Langzeitarchivierung biomedizinischer Forschungsdaten. Workshop Forschungsdatenmanagement in der medizinischen Bildverarbeitung am 29.02.2012 in Magdeburg. Göttingen: Universitätsmedizin; 2012; verfügbar unter http://informatik.med.uni-magdeburg.de/unimagdeburg_mm/Downloads/Institute/IBMI/LABIMIF/Workshop_Forschungsdatenmanagement_01_Dickmann.pdf (aufgerufen 16.8.2012)
18 *Bahmer J*, *Meisel S*, *Hesse B et al.* Projekt zur Erfassung der Einflussfaktoren auf die gutachterliche Leistungsbeurteilung (PEgL) – Chancen sozialmedizinischer Begutachtungsforschung für die Praxis. Med Sach 2010; 106: 255–256
19 *Arbeitsgruppe Erhebung und Nutzung von Sekundärdaten (AGENS) der Deutschen Gesellschaft für Sozialmedizin und Prävention (DGSMP) und der Deutschen Gesellschaft für Epidemiologie (DGEpi)*. GPS – Gute Praxis Sekundärdatenanalyse: Revision nach grundlegender Überarbeitung. 2012; verfügbar unter http://dgepi.de/fileadmin/pdf/GPS_fassung3.pdf (aufgerufen 17.10.2012)
20 *Kampffmeyer U*, *Rogalla J*. Grundsätze der elektronischen Archivierung. „code of practice" zum Einsatz von Dokumenten-Management- und elektronischen Archivsystemen. 2. Aufl. Darmstadt: VOI; 1997

Dieses Dokument wurde zum persönlichen Gebrauch heruntergeladen. Vervielfältigung nur mit Zustimmung des Verlages.