

18 Anhang Teil 1

18.1 Pflichtenheft (Auszug)

18.1.1 Einleitung

Die Vergabe des zu erstellenden Gutachtens zur „Sekundärnutzung medizinischer Behandlungsdaten“ erfolgt im Rahmen des vom BMWi geförderten Projekts cloud4health.⁹⁸⁵ Das vorliegende Pflichtenheft stellt zunächst den Projekthintergrund dar und skizziert die im Projekt adressierten Anwendungsfälle, die beispielhaft für eine ganze Reihe relevanter Szenarien zur Sekundärnutzung klinischer Routinedaten sind. Diese einleitenden Abschnitte sind somit für die Einordnung und das Verständnis des anschließend aufgeführten Fragenkatalogs essentiell.

Ziel des hier beschriebenen Gutachtens ist eine möglichst konkrete und praxisnahe Unterstützung späterer Anwender der vom Projekt cloud4health erarbeiteten Technologien und Methoden zur Sekundärnutzung medizinischer Behandlungsdaten. Entsprechend adressiert der zentrale Abschnitt des eigentlichen Fragenkatalogs die konkreten rechtlichen Rahmenbedingungen eines Anwenders in Abhängigkeit von der Art der medizinischen Einrichtung und des betroffenen Bundeslandes. In Ergänzung zu dem Fragenkatalog sind zudem zu erstellende Mustertexte beschrieben, die ebenfalls die praktische Unterstützung späterer Anwender fokussieren.

[...]

⁹⁸⁵ www.cloud4health.de.

18.1.2 Sekundärnutzung medizinischer Daten im Projekt cloud4health

Die systematische Analyse von bereits vorliegenden medizinischen Behandlungsdaten stellt eine vielversprechende Methode zur Unterstützung der medizinischen Forschung und Qualitätssicherung im Gesundheitsbereich dar. Sowohl national als auch international werden aktuell in einer Vielzahl von Projekten Technologien sowie Organisations- und Verwertungsmodelle entwickelt, die auf den „Rohstoff“ medizinische Behandlungsdaten abzielen und die Sekundärnutzung dieser medizinischen Daten im Sinne einer wissenschaftlichen oder ökonomischen Weiterverwertung außerhalb des Behandlungskontexts anstreben.

Die TMF ist in mehreren Forschungsprojekten beteiligt, die die Sekundärnutzung klinischer Routinedaten zum Gegenstand haben. Hier steht speziell das Projekt „cloud4health“ im Fokus, in dem semantische Technologien zu Produktlösungen integriert werden, mit denen klinische Rohdaten für Sekundärzwecke verfügbar gemacht werden können. Die Rohdaten beinhalten sowohl strukturierte Primärdaten (z.B. Diagnosen, Prozeduren und Labordaten) als auch Daten, die in unstrukturierter oder semi-strukturierter Form vorliegen (z.B. Arztbriefe, Pathologie- und Radiologie-Berichte, Medikationen). Aus unstrukturierten Daten werden mit Hilfe von Textanalyse-Technologien und standardisierten Terminologien relevante Informationen extrahiert, in ein standardisiertes Datenformat überführt und strukturiert abgespeichert. Aus technischer Sicht werden Textanalyse-Technologien und Data-Warehouse-Ansätze miteinander verbunden, wobei der rechenintensive Teil der Datenverarbeitung innerhalb einer Cloud-Infrastruktur⁹⁸⁶ stattfindet. Im Ergebnis können autorisierte Anwender/Forscher auf diese nunmehr strukturierten Daten zugreifen und mit selbst definierten Suchbegriffen recherchieren, um so Erkenntnisse über Ergebnisse verschiedener Behandlungen, Therapien oder neuer medizinischer Anwendungen zu gewinnen.

Die generelle Zielsetzung ist es, mit Hilfe dieser Technologie eine bessere Behandlungsqualität, mehr Sicherheit für die Patienten und eine Kostensenkung im Gesundheitswesen zu erreichen.

18.1.2.1 Beteiligte Akteure und ihre Aufgaben

Krankenhäuser und Arztpraxen: Sie stellen gemäß vorab definierten Einschlusskriterien die relevanten Dokumente (Arztbriefe, OP-Berichte, Laborwerte usw.) aus ihrem Krankenhausinformationssystem (KIS) oder elektronischen Patientenakten zusammen. Mitarbeiter dieser Einrichtungen verarbeiten mit Hilfe spezieller Software die Dokumente soweit vor, dass diese keine direkt personenbezogenen Merkmale mehr aufweisen. Die so anonymisierten oder pseudonymisierten Behandlungsdaten werden zur klinikinternen oder klinikexternen Weiterverarbeitung zur Verfügung gestellt.

Cloud-Provider: Er stellt die Cloud-Infrastruktur zur Verfügung und ist verantwortlich für Sicherheitsmaßnahmen innerhalb der Cloud. Zusammen mit den Kliniken ist er zuständig für die gesicherte Übertragung der Daten von den Kliniken in die Cloud und zurück.

⁹⁸⁶ eine beispielhafte allgemeine Definition findet sich unter: <http://www.cloud.fraunhofer.de/de/faq/cloud.html>.

Software-Hersteller: Er ist Hersteller der beim Cloud-Provider eingesetzten Software und für die Wartung der Software verantwortlich. Ein weiterer Akteur ist Hersteller der in den Kliniken eingesetzten Software. Neben den klinikinternen IT-Administratoren hat er ebenfalls die Aufgabe, diese Software zu warten und zu aktualisieren. Für den ordnungsgemäßen Einsatz der Software in der Klinik muss ggf. von dort auf Ressourcen zugegriffen werden, die im organisatorischen Bereich des Software-Herstellers liegen (z.B. auf Informationen in einer Datenbank).

Forscher/Anwender: Diese Benutzergruppe definiert mit ihren Fragestellungen die Anforderungen an die bereitzustellenden Daten und wertet diese anschließend nach allen Aufbereitungsschritten aus. Sie wird auf eine Nutzungsordnung verpflichtet, die eine zweckgebundene Verwendung vorschreibt und eine Weitergabe der Daten verbietet. Mögliche Nutzer und Anwender der künftigen Infrastruktur sind neben akademisch orientierten Forschern auch Pharmafirmen, Krankenkassen und andere Organe der Selbstverwaltung oder weitere Einrichtungen, die Versorgungsforschung oder Qualitätssicherung betreiben.

Datentreuhänder: Abhängig von der Organisationsstruktur kann es eine vertrauenswürdige Stelle geben, welche die Identifikationsdaten, Zuordnungslisten und Verschlüsselungsalgorithmen verwahrt. Diese vertrauenswürdige Stelle ist rechtlich, räumlich und personell selbstständig und unabhängig. Sie ist regelungsgebunden aber weisungsunabhängig.⁹⁸⁷

Zentrale Organisation: Ebenfalls von der Organisationsstruktur abhängig, kann eine zentrale Organisation die Koordinierung und Bereitstellung der gesamten Infrastruktur übernehmen. Sie ist zentraler Vertragspartner für alle beteiligten Stellen (s. Abb. 1). Die zentrale Organisation stellt in dieser Organisationsstruktur die verantwortliche Stelle dar und fungiert als Auftragnehmer gegenüber dem Kunden (Anwender/Forscher).

18.1.2.2 Datenfluss

Der Datenfluss kann schematisch dem Schaubild in Abbildung 2 entnommen werden.

Die Quelle des Datenflusses liegt in den jeweiligen Kliniken, Krankenhäusern oder Arztpraxen. Anonymisierte oder pseudonymisierte Behandlungsdaten werden in einer Cloud-Infrastruktur aufbereitet und der datenliefernden Stelle in strukturierter Form zurück gespielt. Das Ende des Datenflusses liegt in einem sogenannten Studienportal, in dem diese strukturierten Daten längerfristig abgelegt werden. Hierrüber erfolgt auch der Zugriff der autorisierter Anwender und Forscher. Mit Hilfe der dort zur Verfügung stehenden Software kann diese Benutzergruppe den Datenbestand weiter verarbeiten, durchsuchen und analysieren.

⁹⁸⁷ vergl.:

– Metschke, R., Wellbrock, R. Datenschutz in Wissenschaft und Forschung. 2002. Berliner Beauftragter für Datenschutz und Informationsfreiheit, <http://www.datenschutz-berlin.de/attachments/47/Materialien28.pdf>.

und

– Dierks, C. Rechtsgutachten zur elektronischen Datentreuhänderschaft. 2008. TMF, <http://www.tmf-ev.de/produkte/P052011>

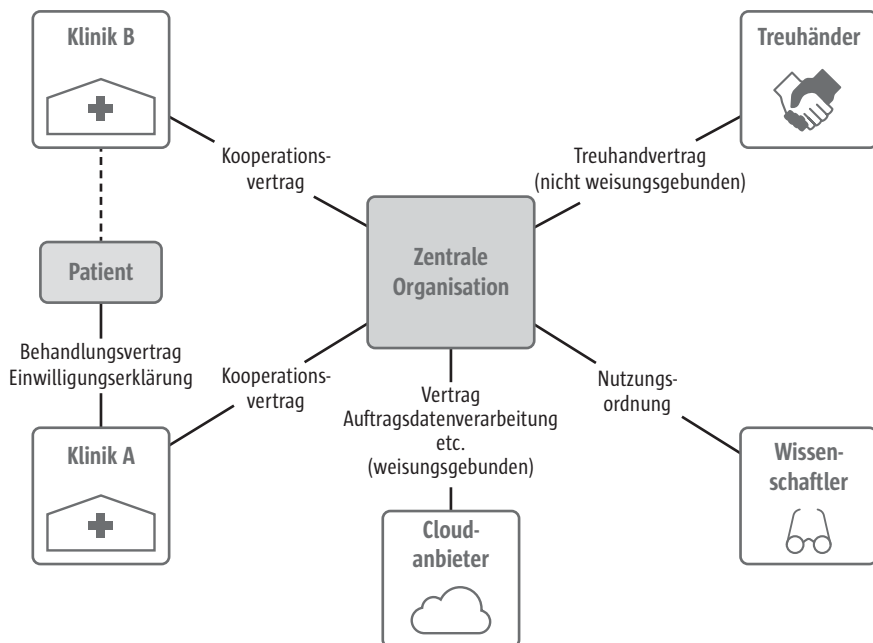


Abb. 1 Exemplarische Struktur der rechtlich-organisatorischen Beziehungen unter Modell 3.

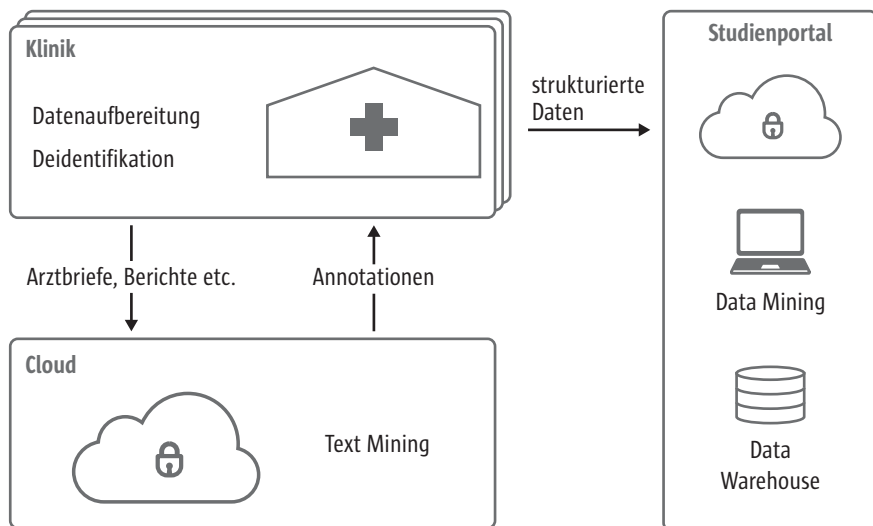


Abb. 2 Verarbeitungsschritte und Datenfluss der medizinischen Behandlungsdaten im Projekt cloud4health

18.1.2.3 Architekturmodelle

Zur Sekundärnutzung medizinischer Behandlungsdaten wurde in dem Projekt cloud4health eine Rahmenarchitektur mit drei unterschiedlichen Modellvarianten entwickelt, die verschiedene Nutzungsszenarien ermöglichen und sich hinsichtlich ihrer Komplexität und Leistungsfähigkeit unterscheiden.

Nach **Modell 1** wird eine hinreichende Anonymisierung der Behandlungsdaten lokal, also innerhalb des Krankenhauses vorgeschaltet, bevor eine Strukturierung durch Text-Mining in einer Cloud-Infrastruktur erfolgt. Die Einholung einer Einwilligung der Patienten ist hier nicht vorgesehen. In diesem Modell ist aufgrund der Anonymisierung die Rückführung der in der Cloud verarbeiteten, strukturierten Behandlungsdaten zu einzelnen Patienten nur unter unverhältnismäßig hohem Aufwand möglich. Um die Anonymität der Daten dauerhaft zu gewährleisten, werden diese in der Cloud nur kurzzeitig gespeichert und verarbeitet und stehen in diesem Zeitfenster nur im Zugriff ausgewählten administrativen Personals des Cloud-Anbieters zu vorgegebenen administrativen Zwecken. Die von den behandelnden Einrichtungen für die weitere Auswertung in das Studienportal hochgeladenen strukturierten Daten werden bei Bedarf ggf. k-anonymisiert.

Im **Modell 2** ist eine klinikinterne Re-Identifizierung ausdrücklich vorgesehen. Im Unterschied zu Modell 1 werden die Behandlungsdaten nicht anonymisiert, sondern pseudonymisiert zur Weiterverarbeitung in die Cloud übermittelt. Nur innerhalb der Klinik existiert ein Schlüssel zur Zuordnung der verarbeiteten Daten zu den einzelnen Patienten, ggf. wird auch die Cloud-Infrastruktur als lokale Cloud innerhalb der behandelnden Einrichtung angesiedelt sein. Ebenso wie in Modell 1 ist die Einholung einer Einwilligung der Patienten nicht vorgesehen. Als Rechtsgrundlage für die pseudonyme Verarbeitung kommen ggf. Landeskrankenhausesetze oder analoge Regelungen in Betracht. Die Aufarbeitung der hierfür in Frage kommenden gesetzlichen Rahmenbedingungen ist zentraler Bestandteil des hier ausgeschriebenen Gutachtens.

Für die Verarbeitung nach **Modell 3** wird eine Einwilligung der Patienten eingeholt. Im Unterschied zu Modell 2 kann die Pseudonymisierung hier klinikübergreifend, unter Einbeziehung einer vertrauensvollen Stelle (Trustee/Treuhänder), die das Pseudonym vergibt und verwaltet, organisiert werden. Dieses Modell gestattet die Rückführbarkeit von Patientendaten und die Nachverfolgung von Patienten im Falle eines Klinikwechsels sowie die Zusammenführung ihrer Daten. Die hierfür notwendige Koordinierung und Bereitstellung der klinikübergreifenden Infrastruktur verantwortet eine zentrale Organisation (siehe auch Kap. I.18.1.2.1 und Abb. 1). Sie steht als verantwortliche Stelle in besonderer Verpflichtung gegenüber den Patienten. Sie erzielt mit ihren Dienstleistungen einen organisatorisch-wirtschaftlichen Mehrwert unter Einhaltung eines klar definierten Aufgabenbereichs und unter Gewährleistung der Rechtskonformität gegenüber den beteiligten Kliniken. Die rechtlichen Voraussetzungen sind hierfür zu prüfen und in Form von Mustertexten zur Vertragsgestaltung zwischen den Beteiligten sicher zu stellen.

18.1.3 Ziele

Das Gutachten „Sekundärnutzung medizinischer Behandlungsdaten“ soll sich in erster Linie an die betroffenen Personen und Institutionen richten, die die Verwendung und den Transfer von Patientendaten zur Sekundärnutzung gesetzeskonform gestalten müssen. Die verantwortlichen Stellen und beteiligten Wissenschaftler eines Forschungs- oder Qualitätssicherungsprojekts sollen mit dem Gutachten in die Lage versetzt werden, alle für ihr Bundesland geltenden gesetzlichen Rahmenbedingungen zu überschauen. Dazu sind alle oben aufgeführten Architekturmodelle mit in die Betrachtung einzubeziehen.

Neben einer Darstellung und Einschätzung des hierbei relevanten gesetzlichen Rahmens sollen daher auch Hinweise und Formulierungshilfen zur Vertragsgestaltung gegeben werden.

18.1.4 Anforderungen an das Gutachten

Die Verarbeitung und Übermittlung von Patientendaten in den Kliniken und Krankenhäusern ist in den einzelnen Bundesländern unterschiedlich geregelt. Die Behandlungsdaten von Patienten sollen über den eigentlichen Behandlungskontext hinaus der Forschung und Qualitätssicherung unter Zuhilfenahme von Cloud Computing zur Verfügung gestellt werden. Für das Gutachten ergeben sich daraus folgende Schwerpunkte:

- Die Vielzahl von Landesdatenschutzgesetzen, Landeskrankenhaus- oder Gesundheitsgesetzen und weiteren spezialgesetzlichen Regelungen erfordert eine Zusammenstellung und Wertung dieser gesetzlichen Grundlagen.
- Das Ziel der Sekundärnutzung erzwingt eine Auseinandersetzung mit den Begriffen „Forschung“ und „Qualitätssicherung“. Eine Abgrenzung der Begriffe untereinander sowie gegenüber dem Zweck der Behandlung erscheint notwendig.
- Die Inanspruchnahme einer Cloud-Infrastruktur und die damit technisch notwendige Datenübermittlung erfordert eine spezifische Berücksichtigung und rechtliche Einordnung dieser Datenverarbeitung, auch in Anbetracht der verschiedenen Möglichkeiten an Vertragsbeziehungen zwischen dem Cloud-Anbieter und der datenübermittelnden Stelle.

Es sind die im Hinblick auf die Nutzung von Behandlungsdaten gemäß den aufgeführten Architekturmodellen auftretenden Rechtsfragen umfassend zu begutachten. Bei der Begutachtung ist die aktuelle Gesetzeslage auf Bundesebene einschließlich internationaler und europarechtlicher Vorgaben sowie die auf Länderebene zu berücksichtigen, untergesetzliche Normen, etwa ärztliches Standesrecht, sind ebenfalls einzubeziehen. Neben den Regelungen zum Datenschutz und zum Umgang mit Gesundheits- und Sozialdaten sind auch weitere Rechtsgebiete zu berücksichtigen, wenn sie für die angesprochenen Anwendungsfälle relevante Bestimmungen enthalten (z.B. TKG, TMG). Die Literatur und Rechtsprechung einschließlich der Spruchpraxis ist umfassend auszuwerten. Bei ungeklärter Rechtslage sind die unterschiedlichen Lösungsansätze und -modelle so darzustellen, dass der Nutzer eine eigene begründete Entscheidung zu treffen vermag. Daneben wird eine Empfehlung des Gutachters erwartet.

Es ist nicht Gegenstand des Gutachtens, im Sozialgesetzbuch (SGB) explizit geregelte Prozesse der Sekundärnutzung durch Sozialleistungsträger oder andere Einrichtungen der Selbstverwaltung zu betrachten. Auch wenn solche im SGB dargestellten Anwendungsfälle von der Begutachtung ausgenommen werden sollen, sind selbstverständlich Bestimmungen des SGB zu berücksichtigen, insofern sie die hier im Fokus stehenden Anwendungsfälle betreffen, diese also ggf. einschränken oder erst ermöglichen.

18.1.4.1 Fragenkatalog

1. Können pseudonymisierte Daten aus Sicht eines Empfängers als anonym gelten, wenn der Sender den Schlüssel für die Pseudonymisierung verwahrt und dieser für den Empfänger nicht zugänglich ist? Geben Sie an, welche Gründe in Literatur und Rechtsprechung für oder gegen die Annahme des Konzepts des relativen Personenbezugs sprechen.
2. Nach welchen Kriterien kann bei der Verwendung von Behandlungsdaten zwischen den Zwecken der Qualitätssicherung und Behandlung getrennt werden? Ab wann und unter welchen Bedingungen wäre die Nutzung zur Qualitätssicherung nicht mehr von der sich aus dem Behandlungsverhältnis ergebenden ursprünglichen Zweckbestimmung umfasst?
3. Wie sieht die datenschutzrechtliche Bewertung eines Vorgangs aus, in dem personenbezogene Daten von einem automatisierten Prozess zu einem anderen Zweck als dem der Behandlung verarbeitet werden und im Ergebnis keine personenbezogenen Daten offenbart werden? Beispielsweise könnte ein solcher Prozess Behandlungsdaten nach passenden Patienten für neue Studien durchsuchen und eine anonyme Fallzahl zurückgeben, anhand derer die Machbarkeit einer Studie mit solchen Patienten abgeschätzt werden könnte. Wäre für eine solche Verarbeitung eine eigene datenschutzrechtliche Rechtsgrundlage erforderlich?
4. Gibt es spezielle Behandlungsdaten, die aufgrund spezialgesetzlicher Regelungen (z.B. GenDG) hinsichtlich ihrer Sekundärnutzung eingeschränkt oder für die besondere Rahmenbedingungen zu berücksichtigen sind? Welche Regelungen sind das und welches sind die zu berücksichtigenden Rahmenbedingungen?
5. Bitte beantworten Sie die folgenden Fragen unter Berücksichtigung vier verschiedener Einrichtungsarten (Krankenhäuser in öffentlicher, privater und kirchlicher Trägerschaft sowie Arztpraxen) und der in den 16 Bundesländern geltenden spezifischen gesetzlichen Rahmenbedingungen. Stellen Sie den jeweils anzuwendenden Rechtsrahmen dar. Nehmen Sie zu jeder der folgenden Fragen jeweils dazu Stellung, ob eine datenschutzrechtliche Einwilligung möglich, nötig oder entbehrlich und ob zusätzlich eine Entbindung von der ärztlichen Schweigepflicht erforderlich ist. Im Folgenden wird der Begriff der Qualitätssicherung so verwendet, dass von einer Zweckänderung gegenüber der Behandlung auszugehen ist (s. Frage 2).
 - 5.1. 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?
 - 5.2. 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.
- 5.3. 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.
 - 5.4. 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?
 - 5.5. 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?
 - 5.6. Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in pseudonymisierter Form im Rahmen einer Datenverarbeitung im Auftrag für Zwecke der Forschung oder Qualitätssicherung übermittelt werden, wenn die behandelnde Einrichtung Auftraggeber ist und
 - 5.6.1. der Auftragnehmer seinen Sitz in Deutschland hat?
 - 5.6.2. der Auftragnehmer seinen Sitz im EU-Ausland hat?
 - 5.7. Unter welchen rechtlichen Bedingungen können die zur Behandlung dokumentierten Daten in pseudonymisierter Form im Rahmen einer in einem Kooperationsvertrag geregelten Funktionsübertragung für Zwecke der Forschung oder Qualitätssicherung an externe Einrichtungen übermittelt werden, wenn Kooperationspartner die behandelnde Einrichtung und
 - 5.7.1. eine externe Einrichtung mit Sitz in Deutschland sind?
 - 5.7.2. eine externe Einrichtung mit Sitz im EU-Ausland sind?
 - 5.8. Unter welchen Bedingungen können die Identitätsdaten der behandelten Patienten zwecks einrichtungsübergreifender Pseudonymisierung an eine zentrale Stelle im Forschungsverbund (z.B. Treuhänder) übermittelt werden.
 - 5.9. Unter welchen Bedingungen sind Ethikkommissionen vor Beginn eines Forschungsprojekts aufgrund der Nutzung personenbezogener oder pseudonymer Daten einzubeziehen? Dabei sollen nur nicht-invasive Studien oder Forschungsprojekte ohne Bezug zum Arzneimittelgesetz oder Medizinproduktegesetz berücksichtigt werden.
 - 5.10. Gibt es Unterschiede hinsichtlich des Forschungszwecks oder der Art der Durchführung eines Forschungsprojekts, die hinsichtlich gesetzlicher Privilegierungen oder Einschränkungen relevant sind (z.B. „zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses“ Art. 27 BayKrG)? Geben Sie Kriterien an, nach denen Forschungsprojekte oder Forschungszwecke hinsichtlich der gesetzlichen Einordnung unterschieden werden können.
 - 5.11. Welche landesspezifischen Unterschiede gibt es hinsichtlich der Ermöglichung von Forschung in besonderen Fällen ohne Einwilligung im Vergleich mit § 28 (6) Nr. 4 BDSG?

- 5.12. Wie grenzen sich die Zuständigkeiten lokaler (behördlicher/betrieblicher) Datenschutzbeauftragter von denen der Aufsichtsbehörden auf Landesebene ab? Welche Kontroll- und Weisungsbefugnisse existieren zwischen diesen? Inwiefern hängen die Zuständigkeiten von den Eigenschaften eines Forschungsprojektes ab (z.B. Verbundforschung)?
- 5.13. Unter welchen rechtlichen Bedingungen ist der Beschäftigtendatenschutz bei der Sekundärnutzung von Behandlungsdaten zu beachten? Auf welcher Ebene müsste in die Verarbeitung personenbezogener Mitarbeiterdaten ggf. eingewilligt werden (z.B. Einrichtungsleitung, Betriebsrat, Betroffene)?
6. Welche zivil- und strafrechtlichen Folgen sind im Falle eines fahrlässigen Datenschutzverstoßes vorgesehen? Geben Sie einen Überblick über die entsprechenden Regelungen des Datenschutzrechts und anderer relevanter Rechtsbereiche. Stellen Sie auch die aktuelle Rechtspraxis dar. Beispielhaft kann eine unerlaubte Re-Identifikation eines betroffenen Probanden mit ggf. sich daraus ergebender Schweigepflichtsverletzung betrachtet werden.

18.2 Abkürzungsverzeichnis

a.A.	anderer Auffassung
ABl.	Amtsblatt
a.F.	alte Fassung
AG	Amtsgericht
AMG	Arzneimittelgesetz
AO	Abgabenordnung
Art.	Artikel
ärztl. geleit.	ärztlich geleitet
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BayKrG	Bayrisches Krankenhausgesetz
BDSG	Bundesdatenschutzgesetz
Begr.	Begründer/Begründung
behörtl.	behördlich
Beschl.	Beschluss
betriebl.	betrieblich
BetrVG	Betriebsverfassungsgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Entscheidung BGH in Strafsachen
BGHZ	Entscheidung des BGH in Zivilsachen
BKK	Betriebskrankenkasse(n)
BMWi	Bundesministerium für Wirtschaft und Energie
BpflV	Bundespflegesatzverordnung
BRAO	Bundesrechtsanwaltsordnung
BSG	Bundessozialgericht
BSGE	Entscheidung des Bundessozialgerichts
bspw.	beispielsweise
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts

BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
CR	Computer und Recht (Zeitschrift)
d.h.	das heißt
dies.	dieselbe/dieselben
Drucks.	Drucksache
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche in Deutschland
DSVO	Datenschutzverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EFTA	European Free Trade Association (Europäische Freihandelsassoziation)
entspr.	entsprechend
Erg.lfg.	Ergänzungslieferung
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EGMR	Europäischer Gerichtshof für Menschenrechte
EWK	Europäischer Wirtschaftsraum
FreihEntzG	Freiheitsentziehungsverfahrensgesetz
GDSG	Gesundheitsdatenschutzgesetz
gem.	gemäß
GenDG	Gendiagnostikgesetz
GesR	Gesundheitsrecht (Zeitschrift)
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GKV	Gesetzliche Krankenversicherung
grds.	Grundsätzlich
HBKG	Heilberufe-Kammergesetz
Hg.	Herausgeber
Hrsg.	Herausgeber
Hs.	Halbsatz
i.d.R.	in der Regel
i.e.S.	im engeren Sinne
i.S.d.	im Sinne des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
juris	Rechtsportal der juris GmbH, u.a. mit Datenbank von Gerichtsentscheidungen

KBV	Kassenärztliche Bundevereinigung
KDO	Katholische Datenschutzverordnung
KG	Kammergericht (Oberlandesgericht in Berlin)
KHDSG	Krankenhausdatenschutzgesetz
KHEG	Krankenhausentwicklungsgesetz
KHEntgG	Krankenhausentgeltgesetzes
KHG	Krankenhausfinanzierungsgesetz
KHGG	Krankenhausgestaltungsgesetz
KLDSG	Krankenhaus-Landesdatenschutzgesetz
Krit.	kritisch
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LKHG	Landeskrankenhausgesetz
LVwG	Landesverwaltungsgesetz
LVwVfG	Landesverwaltungsverfahrensgesetz
m.w.N.	mit weiteren Nachweisen
MBO-Ä	Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
Meldepfl.	Meldepflicht
MedR	Medizinrecht (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
MPG	Medizinproduktegesetz
MVZ	Medizinisches Versorgungszentrum
Nr.	Nummer
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
o.V.	ohne Verfasser
ÖGDG	Gesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
PatDSO	Patientendatenschutzordnung
PharmR	Pharma Recht (Zeitschrift)
PKV	Private Krankenversicherung
PsychKG	Psychisch-Kranken-Gesetz
Rdnr.	Randnummer
RDV	Recht der Datenverarbeitung (Zeitschrift)

s.	siehe
s.o.	siehe oben
s.u.	siehe unten
SGB V	Sozialgesetzbuch V
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TFG	Transfusionsgesetz
TMG	Telemediengesetz
TPG	Transplantationsgesetz
u.ä.	und ähnliches
UBG	Unterbringungsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Dienststelle des Landesbeauftragten für den Datenschutz)
UnterbrG	Unterbringungsgesetz
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
v.a.	vor allem
VerpflG	Verpflichtungsgesetz
VG	Verwaltungsgericht
vgl.	vergleiche
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz

18.3 Verzeichnis der Abkürzungen der Bundesländer

BW	Baden-Württemberg
BY	Bayern
BE	Berlin
BB	Brandenburg
HB	Bremen
HH	Hamburg
HE	Hessen
MV	Mecklenburg-Vorpommern
NI	Niedersachsen
NW	Nordrhein-Westfalen
RP	Rheinland-Pfalz
SL	Saarland
SN	Sachsen
ST	Sachsen-Anhalt
SH	Schleswig-Holstein
TH	Thüringen

18.4 Literaturverzeichnis

- Albrecht, Florian: Datenschutz im Arbeitsverhältnis: Die Neuregelung des § 32 BDSG; juris Praxisreport IT-Recht (jurisPR-ITR) 20/2009 Anm. 2.
- Alkemade, Jan/Blobel, Bernd/Schwanke, Jens/Schütze, Bernd: Der Gehilfe des Arztes – Überlegungen zum Gehilfenbegriff im Sinne des § 203 StGB, Stellungnahme der Arbeitsgruppe „Datenschutz in Gesundheitssystemen“ (DGI) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS); 2003.
- Arning, Marian/Forgó, Nikolaus/Krügel, Tina: Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten; DuD 2006, 700–705.
- Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.
- Artikel-29-Datenschutzgruppe: Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf.
- Bamberger, Heinz-Georg/Roth, Herbert (Hrsg.), BGB, Kommentar, 3. Auflage 2012.
- Bär, Dietrich: Bayrisches Krankenhausgesetz mit Durchführungsverordnung, Kommentar zur Ergänzung, Praxis der Kommunalverwaltung, Band H 10 Bay.
- Becker, Ulrich/Kingreen, Thorsten (Hrsg.): SGB V – Gesetzliche Krankenversicherung – Kommentar, 3. Auflage 2012.
- Bender, Denise: Heilversuch oder klinische Prüfung? Annäherung an eine diffuse Grenze, MedR 2005, 511.
- Berger, Kathrin: Keine Weitergabe von Patientendaten gesetzlich Krankenversicherter an private Dienstleistungsunternehmen zwecks Leistungsabrechnung, Anmerkung zu BSG 6. Senat, Urteil vom 10. Dezember 2008, B 6 KA 37/07 R; jurisPR-ITR 10/2009 Anm. 5.
- Bergmann, Lutz/Möhrle, Roland/Herb, Armin (Hrsg.): Datenschutzrecht, Kommentar; Loseblattausgabe.
- Beyerle, Beatrix: Rechtsfragen medizinischer Qualitätskontrolle, 2004.
- Bizer, Johann: Forschungsfreiheit und informationelle Selbstbestimmung, 1992.
- Bold, Clemens/Sieper, Marc: Landeskrankenhausgesetz Baden-Württemberg, Kommentar, 2012.
- Brisch, Klaus M./Laue, Philip: Zur Weitergabe von Patientendaten an private Abrechnungsstellen als Verletzung der Verschwiegenheitspflicht; CR 2009, 465.
- Caspar, Johannes: Geoinformation und Datenschutz am Beispiel des Internetdienstes Google Street View; DÖV 2009, 965.
- Damm, Reinhard/König, Steffen: Rechtliche Regulierung prädiktiver Gesundheitsinformationen und genetischer „Exzeptionalismus“, MedR 2008, 62.
- Dammann, Ulrich/Simitis, Spiros: EG-Datenschutzrichtlinie, Kommentar, 1997.
- Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo: Bundesdatenschutzgesetz, Kompaktcommentar zum BDSG, 4. Auflage 2013.
- Deutsch, Erwin/Spickhoff, Andreas: Medizinrecht, 7. Auflage, 2014.
- Diener, Holger/Klümper, Mathias: Neufassung der gemeinsamen Empfehlungen von BfArM und PEI zu Anwendungsbeobachtungen veröffentlicht! Was müssen Pharmaunternehmen in der Praxis Neues beachten?, PharmR 2010, 433.
- Eder, Johann/Ciglic, Marga/Koncilia, Christian: ANON: Ein Tool zur Anonymisierung medizinischer Daten. Vortrag auf dem TMF-Jahreskongress 2013, http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=21127&PortalId=0
- Eder, Johann: „k-Anonymität und l-Diversität bieten sicheren Schutz vor dem Ausspionieren personenbezogener Daten“, Interview mit Prof. Dr. Johann Eder über das neue „Anon“-Tool der TMF zur Anonymisierung medizinischer Daten, März 2013; <http://www.tmf-ev.de/News/articleType/ArticleView/articleId/1270.aspx>.
- Ehmann, Eugen: Strafbare Fernwartung in der Arztpraxis, CR 1991, 293.
- Epping, Volker/Hillgruber, Christian (Hrsg.): Grundgesetz, Kommentar, 2. Auflage 2013.
- Erbs, Georg/Kohlhaas, Max: Strafrechtliche Nebengesetze, Beck'sche Kurz-Kommentare, Bd. 17 (BDSG), Loseblattausgabe.
- Fischer, Thomas: Strafgesetzbuch, Kommentar, 61. Auflage 2014.

- Forgó, Nikolaus/Krügel, Tina/Müllenbach, Kathrin: Zur datenschutz- und persönlichkeitsrechtlichen Zulässigkeit von Google Street View; CR 2010, 616.
- Genger, Angie: Das neue Gendiagnostikgesetz; NJW 2010, 113.
- Geppert, Martin/Schütz, Raimund (Hrsg.): Beck'scher TKG-Kommentar, 4. Auflage 2013.
- Gerlach, Carsten: Personenbezug von IP-Adressen, Praktische Konsequenzen aus dem Urteil des LG Berlin vom 31.1.2013; CR 2013, 478.
- Gola, Peter/Jaspers, Andreas: § 32 Abs. 1 BDSG – eine abschließende Regelung?; RDV 2009, 212.
- Gola, Peter/Schomerus, Rudolf: BDSG – Bundesdatenschutzgesetz, Kommentar, 11. Auflage 2012.
- Härtling, Niko: Anonymität und Pseudonymität im Datenschutzrecht; NJW 2013, 2065.
- Hauf, Dietmar: K-Anonymity, I-Diversity and T-Closeness; 2007; http://dbis.ipd.kit.edu/img/content/SS07Hauf_kAnonym.pdf.
- Hauser, Andrea/Haag, Ina: Datenschutz im Krankenhaus, 4. Auflage 2008.
- Heghmans, Michael/Niehaus, Holger: Outsourcing im Versicherungswesen und der Gehilfenbegriff des § 203 III 2 StGB; NSTz 2008, 57.
- Helle, Jürgen/Frölich, Jürgen/Haindl, Hans: Der Heilversuch in der klinischen Prüfung von Arzneimitteln und Medizinprodukten, NJW 2002, 857.
- Henssler, Martin/Willemsen, Heinz J./Kalb, Heinz-Jürgen (Hrsg.): Arbeitsrecht Kommentar, 5. Auflage 2012.
- Hermeler, Angelika-Elisabeth: Rechtliche Rahmenbedingungen der Telemedizin: dargestellt am Beispiel der Elektronischen Patientenakte sowie des Outsourcing von Patientendaten; 2000.
- Hoeren, Thomas/Sieber, Ulrich/Holznapel, Bernd (Hrsg.): Handbuch Multimediarecht, Loseblatt-Ausgabe.
- Hollmann, Angela: Formalmäßige Erklärung über die Entbindung von der Schweigepflicht gegenüber Versicherungsunternehmen; NJW 1978, 2332.
- Honnefelder, Ludger/Propping, Peter (Hrsg.): Was wissen wir, wenn wir das menschliche Genom kennen?, 2001.
- Hornung, Gerrit: Der Personenbezug biometrischer Daten, Zugleich eine Erwiderung auf Saeltzer, DuD 2004, 218ff.; DuD 2004, 429.
- Huster, Stefan/Kaltenborn, Markus (Hrsg.): Krankenhausrecht, Praxishandbuch zum Recht des Krankenhauswesens, 1. Auflage 2010.
- Hustinx, Peter J.: Protection of Personal Data On-Line: The Issue of IP Addresses, 2009; https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf.
- Hustinx, Peter J.: EDPS comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy), 2008; <http://www.statewatch.org/news/2008/sep/ep-eprivacy-edps-opinion.pdf>.
- Joecks, Wolfgang/Miebach, Klaus (Hrsg.): Münchener Kommentar zum Strafgesetzbuch, Band 4, 2. Auflage 2012.
- Kern, Bern-Rüdiger (Hrsg.): Gendiagnostikgesetz, Kommentar, 1. Auflage 2012.
- Kilian, Wolfgang: Rechtsprobleme der Behandlung von Patientendaten im Krankenhaus, Vortrag am 29.04.1985 vor der Saarländischen Krankenhausgesellschaft in Saarbrücken; MedR 1986, 7.
- Kilian, Wolfgang/Heussen, Benno: Computerrechts-Handbuch, Loseblatt-Ausgabe.
- Klar, Manuel: Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012.
- Klar, Manuel: Privatsphäre und Datenschutz in Zeiten technischen und legislativen Umbruchs; DÖV 2013, 103.
- Köpke, Jan: Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für private Krankenversicherer, insbesondere bei der innerorganisatorischen Geheimnisweitergabe; 2003; <http://hdl.handle.net/10900/43694>.
- Kroschwald, Steffen: Verschlüsseltes Cloud Computing, Auswirkungen der Kryptografie auf den Personenbezug in der Cloud; ZD 2014, 75.
- Krüger, Stefan/Maucher, Svenja-Ariane: Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis; MMR 2011, 433.
- Krauskopf, Dieter (Begr.): Soziale Krankenversicherung, Pflegeversicherung, Kommentar, Loseblattausgabe.
- Kügel, J. Wilfried/Müller, Rolf-Georg/Hofmann, Hans-Peter (Hrsg.): Arzneimittelgesetz, Kommentar, 1. Auflage 2012.
- Kühling, Jürgen/Klar, Manuel: Datenschutz bei E-Health – Zeit für grundlegende Reformen; DuD 2013, 791.

- Kühling, Jürgen/Klar, Manuel: Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität; NJW 2013, 3611.
- Kühling, Jürgen/Seidel, Christian: Abrechnung von Gesundheitsleistungen durch Private nach dem ASNEF-Urteil des EuGH – „Novemberrevolution“ im Datenschutz?; GesR 2012, 402.
- Lackner, Karl/Kühl, Kristian: StGB, Kommentar, 27. Auflage 2011.
- Laufhütte, Heinrich-Wilhelm/Rissing-van Saan, Ruth/Tiedemann, Klaus (Hrsg.), Leipziger Kommentar zum StGB, 11. Auflage 2005.
- Leitherer, Stephan (Hrsg.): Kasseler Kommentar zum Sozialversicherungsrecht, Loseblattausgabe.
- Leupold, Andreas/Glossner, Silke: Münchener Anwaltshandbuch IT-Recht, 2. Auflage 2011.
- LfD Bayern (Landesbeauftragter für den Datenschutz in Bayern): Orientierungshilfe: Pseudonymisierung in der medizinischen Forschung, Stand 29.11.2005; www.datenschutz-bayern.de.
- LfD Baden-Württemberg (Landesbeauftragter für den Datenschutz in Baden-Württemberg): 2. Tätigkeitsbericht, 1981.
- LfD Hessen (Der Hessische Datenschutzbeauftragte): 29. Tätigkeitsbericht, 2000; abrufbar unter <http://www.datenschutz.hessen.de/taetigkeitsberichte.htm>.
- LfD Hessen (Der Hessische Datenschutzbeauftragte): 30. Tätigkeitsbericht, 2001; abrufbar unter <http://www.datenschutz.hessen.de/taetigkeitsberichte.htm>.
- LfD Niedersachsen (Der Landesbeauftragte für den Datenschutz Niedersachsen), Das Niedersächsische Datenschutzgesetz, Gesetzestext und Kommentar, Stand: März 2014; http://www.lfd.niedersachsen.de/download/32433/NDSG_mit_Kommentar_Stand_07.03.2014_.pdf.
- LfD Nordrhein-Westfalen (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen): 17. Datenschutz- und Informationsfreiheitsbericht, Berichtszeitraum: 01.01.2003 – 31.12.2004, vorgelegt 2005.
- Lippert, Hans-Dieter: Änderungen im AMG und in der MBOÄ, Welche Auswirkungen ergeben sich daraus für die Arbeit der Ethikkommission?, GesR 2012, S. 467.
- Listl, Susanne: Die zivilrechtliche Haftung von für Fehler von Ethikkommissionen, 2012.
- Lorenz, Sylvia: Datenschutzrechtliche Einordnung der IP-Adresse („Speicherung dynamischer IP-Adressen“), Anmerkungen zu BGH 3. Zivilsenat, Urteil vom 13.01.2011 – III ZR 146/10, jurisPR-ITR 15/2011 Anm. 2
- Masing, Johannes: Herausforderungen des Datenschutzes; NJW 2012, 2305.
- Meier, Andre: Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003.
- Menzel, Hans-Joachim: Brennpunkt: Datenschutz – DNA-Analysedaten, Die rechtliche Sicht, in: Sokol, Bettina (Hg.): Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz, 2003.
- Metschke, Rainer/Wellbrock, Rita: Datenschutz in Wissenschaft und Forschung, 3. Auflage 2002; http://www.datenschutz.hessen.de/download.php?download_ID=61&download_now=1.
- Meyerdierks, Per: Sind IP-Adressen personenbezogene Daten? MMR 2009, 9.
- Meyerdierks, Per: Personenbeziehbarkeit statischer IP-Adressen, Datenschutzrechtliche Einordnung der Verarbeitung durch Betreiber von Webseiten; MMR 2013, 705.
- Moos, Flemming: Die Entwicklung des Datenschutzrechts im Jahr 2007; K & R 2008, 137.
- Mrozynski, Peter: Sozialgesetzbuch – Allgemeiner Teil (SGB I), Kommentar, 4. Auflage 2010.
- Münchener Kommentar zum Strafgesetzbuch: StGB, hrsg. von Wolfgang Joecks, Band 4: §§ 185–262 StGB, 2. Auflage 2012.
- Nell, Ernst Ludwig: Wahrscheinlichkeitsurteile in juristischen Entscheidungen, 1983.
- Ohne Verfasser: BKK Gesundheit: Unbekannter fordert zum „Daten-Ankauf“ auf; heise news, 11.02.2010; <http://www.heise.de/newsticker/meldung/BKK-Gesundheit-Unbekannter-fordert-zum-Daten-Ankauf-auf-928649.html>.
- Ohne Verfasser: Brüssel unterstützt Merkels Vorstoß für „Schengen-Netz“; heise news, 17.02.2014; <http://www.heise.de/newsticker/meldung/Bruessel-unterstuetzt-Merkels-Vorstoss-fuer-Schengen-Netz-2116663.html>.
- Pahlen-Brandt, Ingrid: Zur Personenbezogenheit von IP-Adressen, Zugleich eine Replik auf Eckhardt, K & R 2007, 602ff.; K & R 2008, 288.
- Palandt, Otto (Begr.): Bürgerliches Gesetzbuch mit Nebengesetzen, Kommentar, 73. Auflage 2014.

- Paul, Jörg-Alexander/Gendele, Boris: Outsourcing von Krankenhausinformationssystemen, Praxishinweise zur rechtskonformen Umsetzung; ZD 2012, 315.
- Plath, Kai-Uwe (Hrsg.): Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, 2013.
- Pöttgen, Nicole: Medizinische Forschung und Datenschutz, 2008.
- Prütting, Dorothea (Hg.): Fachanwaltskommentar Medizinrecht, 3. Auflage, 2014.
- Ramos, Thanos: Kontaktlose Zahlungen mittels mobiler Endgeräte, The future is near ... field communication? – Datenschutzrechtliche Rahmenbedingungen; ZD 2013, 599.
- Raspe, Heiner/Hüppe, Angelika/Strech, Daniel/Taupitz, Jochen: Empfehlungen zur Begutachtung klinischer Studien durch Ethik-Kommissionen, 2. Auflage 2012.
- Ratzel, Rudolf/Lippert, Hans-Dieter: Kommentar zur Musterberufsordnung der deutschen Ärzte (MBO), 5. Auflage 2010.
- Ratzel, Rudolf/Lippert, Hans-Dieter: Das Berufsrecht der Ärzte nach den Beschlüssen des 114. Deutschen Ärztetages in Kiel; GesR 2011, 536.
- Redeker, Helmut: IT-Recht, NJW-Praxis Band 55, 5. Auflage 2012.
- Rehmann, Wolfgang: Arzneimittelgesetz (AMG), Kommentar, 3. Auflage, 2008.
- Richardi, Reinhard (Hrsg.): Betriebsverfassungsgesetz mit Wahlordnung, Kommentar, Beck'sche Kommentare zum Arbeitsrecht, 14. Auflage 2014.
- Rolfs, Christian/Giesen, Richard Leo Ernst/Kreikebohm, Ralf/Udsching, Peter (Hrsg.): Beck'scher Online-Kommentar Sozialrecht.
- Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht, 2003.
- Roßnagel, Alexander: Datenschutz in der künftigen Verkehrstelematik; NZV 2006, 281.
- Roßnagel, Alexander/Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten; MMR 2000, 721.
- Sander, Axel: Arzneimittelrecht, Kommentar für die juristische Praxis zum Arzneimittelgesetz, Loseblattausgabe.
- Saeltzer, Gerhard: Sind diese Daten personenbezogen oder nicht?, Wie der Personenbezug von Daten, auch biometrischer, sich fundiert prüfen lässt ...; DuD 2004, 218.
- Schaar, Peter: Datenschutz im Internet, 2002.
- Schaffland, Hans-Jürgen/Wiltfang, Noeme: Bundesdatenschutzgesetz (BDSG), Ergänzbare Kommentar nebst einschlägigen Rechtsvorschriften.
- Schillhorn, Kerrin/Heidemann, Simone: Gendiagnostikgesetz, Kommentar für die Praxis, 2011.
- Schlegel, Thomas: KBV beansprucht Monopol – zu Recht? Abrechnung ärztlicher Leistungen; Der Kassenarzt 2009, 36.
- Schmidt, Bernd: Arbeitnehmerdatenschutz gemäß § 32 BDSG – Eine Neuregelung (fast) ohne Veränderung der Rechtslage; RDV 2009, 193.
- Schmidt, Georg/Seiler, Christoph/Maier, Petra/Vollmöller, Thomas: Thüringer Krankenhausgesetz, Kommentar zur Ergänzung, Praxis der Kommunalverwaltung, Band H 10 Th.
- Schneider, Uwe K.: Abrechnungsstellen und Datenschutz in der GKV, Das Urteil des BSG vom 10.12.2008 und die Folgeänderungen im Rahmen der 15. AMG-Novelle; VSSR 2009, 381.
- Schneider, Uwe K.: Datenschutz in der vernetzten Medizin; Grätzel von Grätz (Hg.), Vernetzte Medizin, 2004, S. 136.
- Schönke, Adolf/Schröder, Horst: StGB, Kommentar, 28. Auflage 2010.
- Schott, Gisela/Pachl, Henry/Limbach, Ulrich/Gundert-Remy, Ursula/Ludwig, Wolf-Dieter/Lieb, Klaus: Finanzierung von Arzneimittelstudien durch pharmazeutische Unternehmen und die Folgen; Teil 1: Qualitative systematische Literaturübersicht zum Einfluss auf Studienergebnisse, -protokoll und -qualität, DÄ Int. 2010, S. 279–285; Teil 2: Qualitative systematische Literaturübersicht zum Einfluss auf Autorschaft, Zugang zu Studiendaten sowie auf Studienregistrierung und Publikation, DÄ Int. 2010, S. 295–301.
- Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz Kommentar, 8. Auflage 2014.
- Sokol, Bettina (Hrsg.): Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz, 2003.
- Sosnitz, Olaf/Op den Camp, Albert: Auswirkungen des Gendiagnostikgesetzes auf klinische Prüfungen; MedR 2011, 401.
- Specht, Louisa/Müller-Riemenschneider, Severin: Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber? Aktueller Stand der Diskussion um den Personenbezug; ZD 2014, 71.

- Spickhoff, Andreas (Hrsg.): Medizinrecht, Kommentar, 1. Auflage 2011.
- Spindler, Gerald/Schuster, Fabian: Recht der elektronischen Medien, 2. Auflage 2011.
- Steinsbekk, Kristin Solum/Myskja, Bjørn Kåre/Solberg, Berge: Broad consent versus dynamic consent in biobank research, *European Journal of Human Genetics* 2013, 897.
- Sweeney, Latanya: Simple Demographics Often Identify People Unique; Carnegie Mellon University, Data Privacy Working Paper 3, 2000; <http://dataprivacylab.org/projects/identifiability/paper1.pdf>.
- Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Kommentar, 2. Auflage 2013.
- Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) (Hrsg.): Rechtsgutachten zum Datenschutz in der medizinischen Forschung; 2009; http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=1424&PortalId=0.
- Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) (Hrsg.): Jahresbericht 2013; http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=24237&PortalId=0.
- Taupitz, Jochen: Humangenetische Diagnostik zwischen Freiheit und Verantwortung: Gentests unter Arztvorbehalt; Honnefelder, Ludger/Propping, Peter (Hg.): Was wissen wir, wenn wir das menschliche Genom kennen? 2001.
- Thüsing, Gregor: Datenschutz im Arbeitsverhältnis, Kritische Gedanken zum neuen § 32 BDSG; NZA 2009, 865.
- Trittin, Wolfgang/Fischer, Esther: Datenschutz und Mitbestimmung, Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung; NZA 2009, 343.
- ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): Verbotsverfügung gegenüber dem Hausärzterverband Schleswig-Holstein, Anordnung vom 21.07.2010, <https://www.datenschutzzentrum.de/medizin/gkv/20100721-verfuegung-hzv.html>.
- ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): Patientendatenschutz im Krankenhaus; <https://www.datenschutzzentrum.de/medizin/kranken/patdskh.htm#11>.
- Voigt, Paul: Gesprächsaufzeichnung im Servicecallcenter – Opt-In oder Opt-Out? Eine datenschutzrechtliche Betrachtung; DuD 2008, 780.
- Voigt, Paul: Datenschutz bei Google; MMR 2009, 377.
- Vogeler, Marcus: Ethik-Kommissionen – Grundlagen, Haftung und Standards, 2011.
- Vossenkuhl, Cosima: Der Schutz genetischer Daten unter besonderer Berücksichtigung des Gendiagnostikgesetzes, Schriftenreihe Medizinrecht, 2013.
- Weichert, Thilo: Datenschutzrechtliche Probleme in der sektorenübergreifenden Qualitätssicherung, VSSR 2010, 227.
- Weichert, Thilo: Aktuelle Herausforderungen des Datenschutzes im Bereich der medizinischen Forschung, Zusammenfassung des Vortrages auf dem 4. TMF-Jahreskongress am 28.03.2012 in Kiel; 2012; <https://www.datenschutzzentrum.de/vortraege/20120328-weichert-medizinische-forschung.html>.
- Wolff, Heinrich Amadeus/Brink, Stefan: Beck Online Kommentar BDSG.
- Wuermeling, Ulrich: Scoring von Kreditrisiken; NJW 2002, 3508.

Hinweis zu den zitierten Webseiten:

Sämtliche zitierten Webseiten wurden am 16.03.2015 überprüft und hatten zu diesem Zeitpunkt den zu belegenden Inhalt.