I

Sekundärnutzung medizinischer Behandlungsdaten

Uwe K. Schneider[1]

1 Der Autor dankt Dr. Manuel Klar für seine Mitarbeit an den Kapiteln I.2, I.3, I.4 und I.16 sowie Johannes Bernhardt für seine Mitarbeit an den Kapiteln I.5 und I.11.

Inhalt Teil I

1 Vorwort 9

2 Personenbezug bei Pseudonymisierung und Anonymisierung 11

2.1 Relativität des Personenbezugs in subjektiver Hinsicht 12
2.1.1 Überblick 12
2.1.2 Stellungnahme 14

2.2 Relativität des Personenbezugs in objektiver Hinsicht 17
2.2.1 Datenschutzrechtliche Anforderungen an eine faktische Anonymisierung 17
2.2.2 Methoden der Anonymisierung 20
2.2.3 Empfehlungen zur Risikovorsorge 23

2.3 Ergebnis 24

3 Abgrenzung der Verarbeitungszwecke „Qualitätssicherung“ und „Behandlung“ 25

3.1 Typische Behandlungszwecke 26

3.2 Typische Zwecke der Qualitätssicherung 27

3.3 Abgleich der Zwecke: komplementärer Anwendungsbereich oder Überschneidungsbereiche? 27

3.4 Ergebnis 28

4 Zweckändernde automatisierte Auswertung personenbezogener Daten mit anonymen Ergebnissen 31

4.1 Bewertung aus Sicht des Datenschutzrechts im engeren Sinne 32
4.1.1 Umgang mit „personenbezogenen Daten“ trotz anonymen Outputs? 32
4.1.2 Hilfsweise: Bedeutung einer Zweckänderung im Datenschutzrecht 41

4.2 Vereinbarkeit mit der Schweigepflicht der Heilberufe 47
4.2.1 Verletzung von Privatgeheimnissen (§ 203 StGB) 47
4.2.2 Berufsrechtliche Verschwiegenheitspflicht (§ 9 Abs. 1 MBO-Ä) 51

4.3 Ergebnis 51

5 Spezialgesetzliche Einschränkungen der Sekundärnutzung 53

5.1 Bundeseinheitliche Regelungen 53
5.1.1 Gendiagnostikgesetz (GenDG) 53
5.1.2 Transplantationsgesetz (TPG) 60
5.1.3 Medizinproduktegesetz (MPG) 61
5.1.4 Transfusionsgesetz (TFG) 62
5.1.5 Arzneimittelgesetz (AMG) 64

5.2 Länderspezifische Regelungen bei Unterbringung psychisch Kranker 69
5.2.1 Länder ohne spezifische Regeln 70
5.2.2 Sonderregeln zum Datenschutz 70
5.2.3 Sonderregelungen zur Forschung mit personenbezogenen Daten 72

6 Anwendbares Datenschutzrecht für die Sekundärnutzung klinischer Daten unter Berücksichtigung des Landesrechts 75

6.1 Verhältnis von Datenschutz und Schweigepflicht 75

6.1.1 Unabhängigkeit von Datenschutz und Schweigepflicht (Zwei-Schranken-Theorie) 76

6.1.2 Besondere Zweckbindung nach Übermittlung aufgrund der Schweigepflicht 77

6.2 Eingeschränkte Sonderregeln für Religionsgemeinschaften 80

6.3 Übersicht 1: Auf Krankenhäuser anwendbares Datenschutzrecht und Datenschutzaufsicht 81

6.4 Übersicht 2: Gesetzliche Erlaubnisse zur Sekundärnutzung von Behandlungsdaten 87

6.5 Bundesdatenschutzgesetz 90

6.5.1 Anwendungsbereich 90

6.5.2 Forschungsklausel (§ 28 Abs. 6 Nr. 4 BDSG) 93

6.5.3 Qualitätssicherung 108

6.5.4 Einwilligung 110

6.6 Für Kliniken relevante Datenschutzvorschriften der Bundesländer 123

6.6.1 Baden-Württemberg 123

6.6.2 Bayern 135

6.6.3 Berlin 143

6.6.4 Brandenburg 151

6.6.5 Bremen 156

6.6.6 Hamburg 162

6.6.7 Hessen 167

6.6.8 Mecklenburg-Vorpommern 172

6.6.9 Niedersachsen 178

6.6.10 Nordrhein-Westfalen 183

6.6.11 Rheinland-Pfalz 188

6.6.12 Saarland 195

6.6.13 Sachsen 206

6.6.14 Sachsen-Anhalt 213

6.6.15 Schleswig-Holstein 217

6.6.16 Thüringen 221

6.7 Für Kliniken relevante Datenschutzvorschriften der Kirchen 229

6.7.1 Evangelische Kirche 229

6.7.2 Katholische Kirche 233

7 Verwendung von Behandlungsdaten für interne Qualitätssicherung und Eigenforschung 239

7.1 Verwendung von Behandlungsdaten in unveränderter Form durch den Behandler 239

7.1.1 Zweckänderung hin zur Forschung 240

7.1.2 Zweckänderung hin zur Qualitätssicherung 246

7.2 Verwendung von Behandlungsdaten in pseudonymisierter Form durch den Behandler 249
7.2.1 Verwendung pseudonymer Daten durch den Behandler 249
7.2.2 Vorgang der Pseudonymisierung 250
7.3 Verwendung von Behandlungsdaten in anonymisierter Form durch den Behandler 251
7.3.1 Verwendung anonymer Daten durch den Behandler 251
7.3.2 Vorgang der Anonymisierung 251
7.4 Verwendung von Behandlungsdaten in pseudonymisierter Form durch nicht behandelndes Personal in der gleichen Fachabteilung 253
7.4.1 Personenbezogene Datenverwendung der Behandlungseinrichtung 253
7.4.2 Kein besonders rechtfertigungsbedürftiges Übermitteln, aber rechtfertigungsbedürftige sonstige Verwendung 254
7.5 Verwendung von Behandlungsdaten in pseudonymisierter Form durch Personal anderer Fachabteilungen 255
7.5.1 Personenbezogene Datenverwendung der Behandlungseinrichtung 255
7.5.2 Teils besonders rechtfertigungsbedürftiges Übermitteln, teils rechtfertigungsbedürftige sonstige Verwendung 255

8 Datenverarbeitung im Auftrag für Zwecke der Forschung oder Qualitätssicherung 259

8.1 Allgemeine Einordnung der Auftragsdatenverarbeitung im Kontext der Sekundärnutzung 259
8.1.1 Zulässigkeit der Forschung oder Qualitätssicherung durch die Behandlungseinrichtung 259
8.1.2 Personenbezug für den Auftragnehmer? 260
8.1.3 Offenbaren im Sinne der Schweigepflicht (§ 203 StGB) 262
8.1.4 Allgemeine Charakteristika der Auftragsdatenverarbeitung 264
8.1.5 Fehlender Personenbezug: Entbehrlichkeit einer besonderen Erlaubnis, Sinnhaftigkeit vertraglicher Absicherungen 265
8.2 Gesundheitsspezifische Regelungen zur Auftragsdatenverarbeitung 266
8.2.1 Keine gesundheitsspezifische Auftragsdatenverarbeitung im BDSG 267
8.2.2 Landeskrankenhaus- oder vergleichbare Gesetze 267
8.3 Zusammenfassende Bewertung 280

9 Übermittlung pseudonymer Daten im Wege der Funktionsübertragung für Forschung oder Qualitätssicherung 283

9.1 (Kein) Personenbezug für die externe Einrichtung 283
9.2 Zulässigkeit der „Übermittlung" sowie von interner Vor- und Nachbereitung 284
9.2.1 Keine Übermittlung mangels Personenbezug für die externe Einrichtung 284
9.2.2 Übermittlung bei angenommenem Personenbezug für die externe Einrichtung 284
9.3 Übersicht 5: Explizite gesetzliche Anforderungen an Übermittlungsempfänger 286

10 Einrichtungsübergreifende Pseudonymisierung im Forschungsverbund 289

10.1 Identitätsdaten als personenbezogene Gesundheitsdaten bzw. Patientengeheimnisse 289

10.2 Funktionsübertragung und Eigenverantwortlichkeit des Datentreuhänders 290

10.3 Zulässigkeit 291

10.3.1 Regelungen ohne Offenbarungsbefugnis 291

10.3.2 Vorhabenbezogene Erlaubnisnormen für die Datenübermittlung 292

10.3.3 Einrichtungsübergreifende Pseudonymisierung aufgrund Einwilligung 292

10.4 Vertragliche Ausgestaltung 293

11 Einbeziehung von Ethikkommissionen bei Forschung mit personenbezogenen oder pseudonymen Daten 295

11.1 Einbeziehung von Ethikkommissionen nach § 15 MBO-Ä 295

11.1.1 Pflicht zur Einbeziehung einer Ethikkommission 295

11.1.2 Zusammensetzung der Ethikkommission 296

11.1.3 Zuständigkeit und Verfahren 296

11.1.4 Rechtliche Einordnung der Bewertung 298

11.2 Zum Begriff des Personenbezugs in § 15 MBO-Ä 298

11.2.1 Vorüberlegungen 298

11.2.2 Begriff des Personenbezugs in § 15 MBO-Ä 299

11.2.3 Ergebnis: Grundsätzlich gleiche Bedeutung des Personenbezugs in § 3 Abs. 1 BDSG und § 15 Abs. 1 MBO-Ä 303

11.3 Abgleich mit den Berufsordnungen der Landesärztekammern 304

11.3.1 Landesärztekammern ohne eine Neufassung des § 15 BO 304

11.3.2 Landesärztekammern mit einer Neufassung des § 15 der Berufsordnung 305

12 Für die Sekundärnutzung relevante Unterschiede hinsichtlich Forschungszweck und Art der Durchführung eines Forschungsvorhabens 307

13 Landesspezifische und für die Sekundärnutzung relevante Unterschiede in den Forschungsklauseln 309

13.1 Grundlegende Unterschiede 309

13.2 Übersicht 6: Unterschiede zwischen den Forschungsklauseln im Einzelnen 310

14 Datenschutzbeauftragte und Aufsichtsstrukturen 315

14.1 Zuständigkeiten der lokalen Datenschutzbeauftragten 315

14.2 Zuständigkeiten der Beauftragten für den Datenschutz des Bundes und der Länder sowie der Aufsichtsbehörden auf Landesebene 316

14.2.1 Datenschutzbeauftragte des Bundes und der Länder 317

14.2.2 Aufsichtsbehörden der Länder nach § 38 BDSG 318

14.3 Zuständigkeiten bei Verbundforschung 319

15 Beschäftigtendatenschutz bei der Sekundärnutzung von Behandlungsdaten 321

15.1 Übersicht 7: Auf Beschäftigungsverhältnisse in Kliniken vorrangig anwendbares Datenschutzrecht 323

15.2 Anwendungsbereich des BDSG 324

15.2.1 Datenschutzrechtliche Erlaubnis 324

15.2.2 Exkurs: Mitbestimmung bei möglicher Leistungs- oder Verhaltenskontrolle 329

15.3 Anwendungsbereich der Landesdatenschutzgesetze 330

15.4 Anwendungsbereich der kirchlichen Datenschutzgesetze 331

15.4.1 Kliniken der evangelischen Kirche 331

15.4.2 Kliniken der katholischen Kirche 332

16 Zivil- und strafrechtliche Folgen fahrlässiger Datenschutzverstöße 335

16.1 Zivilrechtliche Folgen 336

16.1.1 § 7 BDSG – Verschuldensabhängige Haftung 336

16.1.2 § 8 BDSG – Gefährdungshaftung für öffentliche Stellen 337

16.1.3 § 823 Abs. 1 und 2 BGB – Verschuldensabhängige Haftung 338

16.1.4 § 280 Abs. 1 in Verbindung mit § 241 Abs. 2 BGB – Vertragliche Haftung 338

16.1.5 Sonstige Haftungsnormen 339

16.2 Strafrechtliche Folgen 339

16.2.1 Abgrenzung: Bedingter Vorsatz und bewusste Fahrlässigkeit 339

16.2.2 Abgrenzung: Normativer Verbotsirrtum und faktische Fahrlässigkeit 339

16.3 Ergebnis 340

17 Rechtspolitisches Schlusswort 343

18 Anhang Teil 1 347

18.1 Pflichtenheft (Auszug) 347

18.1.1 Einleitung 347

18.1.2 Sekundärnutzung medizinischer Daten im Projekt cloud4health 348

18.1.3 Ziele 352

18.1.4 Anforderungen an das Gutachten 352

18.2 Abkürzungsverzeichnis 356

18.3 Verzeichnis der Abkürzungen der Bundesländer 360

18.4 Literaturverzeichnis 361

1 Vorwort

Medizinische Daten können auch über den primären Behandlungskontext, in dem sie erhoben wurden, hinaus erheblichen Nutzen stiften. So kann ihre Auswertung zeigen, ob und inwieweit bestehende Qualitätsstandards in einer Behandlungseinrichtung oder im Gesundheitswesen allgemein beachtet werden, was deren Einhaltung längerfristig sichert. Zudem können auf dieser Datenbasis Hypothesen generiert und überprüft werden, was die Erforschung neuer Behandlungsmethoden unterstützt.

Je größer die analysierten Datenmengen, desto valider sind in der Regel die dabei gewonnenen Erkenntnisse. Mit dem Text- und Data-Mining stehen grundsätzlich Methoden zur Verfügung, um der inhaltlichen Komplexität einer solchen „Big Data"-Analyse gerecht zu werden. Durch das Text-Mining können dabei un- oder schwach strukturierte Dokumente (z.B. Freitext-Arztbriefe) semantisch analysiert und geordnet werden. So strukturierte Daten können mittels des Data-Mining weiter ausgewertet werden. Die Anwendung dieser Methoden auf große Datenmengen ist zwar rechenintensiv, mit der Cloud-Technologie existiert jedoch eine Möglichkeit zur effizienten Nutzung gegebenenfalls auch weit verteilter IT-Ressourcen.

Diesem Nutzenpotential stehen aber auch Risiken gegenüber, wenn Behandlungsdaten aus der Vertrauensbeziehung zwischen Arzt und Patient, die dem Zweck der Behandlung dient, herausgelöst und für die sekundären Zwecke der Qualitätssicherung oder Forschung gegebenenfalls in weit verteilten Strukturen verwendet werden. Die Kontrolle der tatsächlichen Einhaltung des vorgegebenen Zweckrahmens wird durch eine entsprechende Datenverteilung erschwert. Dies kann zudem dazu führen, dass die betroffenen Patienten unter Umständen innerhalb des Gesundheitswesens