vogel & partner
rechtsanwälte

Datenschutz und Smart Health Data

Smart Data – Smart Privacy – Smart Healthcare

Begleitforschung zum BMWi-Technologieprogramm Smart Data
Impulsreferat für den Vernetzungsworkshop Gesundheit
Berlin, 27.01.2016

Dr. Uwe K. Schneider
Rechtsanwalt
Fachanwalt für Medizinrecht

Smart Data

Big Data

- Big Volume, Big Variety, Big Velocity
- oft Zusammenführung aus unterschiedlichen Quellen (in Data Warehouse)
- oft Auswertung zu verschiedenen Zwecken (Data Mining)
- oft ergebnisoffene Hypothesengenerierung

Smart Data

- intelligente Anwendung von Big Data, so dass Daten Sinn ergeben
- nicht unbedingt Masse (Big), sondern wertvolle Inhalte / Zusammenhänge (Smart)
- teils auf Auswertung der Daten, die „smart devices“ (Geräte/Anlage) liefern, bezogen

Smart Health Data

- Anwendung von Smart Data auf Gesundheitsdaten
- InnOpPlan: Innovative, datengetriebene Effizienz OP-übergreifender Prozesse
- KDI: Klinische Datenintelligenz (Daten direkt aus Behandlung, med. Geräten, …)
- SAHRA: Auswertung von Abrechnungsdaten der Krankenkassen

Privacy & Health Data

Geltendes Datenschutzrecht (Grundsätze)

- Verbot mit Erlaubnisvorbehalt: gesetzliche Erlaubnis od. Einwilligung d. Betroffenen
- Zweckbindung: Erlaubnis nur für die im Gesetz oder Einwilligung bestimmten Zwecke
- Erforderlichkeit (Datensparsamkeit): nur f. den Zweck notwendige Daten verarbeiten
- Transparenz der Verarbeitung für den Betroffenen
- Sicherheit der Datenverarbeitung
- besonderer Schutz für Gesundheitsdaten (v.a. grds. Verbot & Zweckbindung streng)

Schweigepflicht in der Medizin

- für Angehörige von Heilberufen, deren Einrichtungen (Kliniken) & (interne) Gehilfen
- unbefugtes Offenbaren von Patientendaten ist strafbar (§ 203 StGB)
- Befugnis zum Offenbaren (an Dritte wie Ärzte in anderen Klinken, Dienstleister)
  - Gesetz, das sich auf das Arzt-Patienten-Verhältnis bezieht (nicht BDSG)
  - Entbindung durch den Patienten (entspricht Einwilligung)
- Hürde für (einrichtungsübergreifende) Kooperation & Outsourcing bei Big Data

Big Data – Poor Privacy?

Bindung an Erhebungszwecke

- Zweckänderung bedarf neuer Rechtfertigung: Gesetz oder Einwilligung
- Besonders streng bei Daten aus dem Vertrauensverhältnis zw. Arzt & Patient

↯ Auswertung für überindividuelle und vielfältige Zwecke

Bestimmtheit der Zwecke

↯ automatisierte Suche nach unbekannten Zusammenhängen

Erforderlichkeit/Datensparsamkeit

↯ je mehr Daten, desto besser (auf Vorrat oder wegen besserer Analyseergebnisse)

Smart Privacy?

Kritik am heutigen Datenschutz

- Merkel: Datenschutz darf Big Data nicht verhindern (Nationaler IT-Gipfel 2015)
- Dobrindt: Datenreichtum statt Datensparsamkeit (Nationaler IT-Gipfel 2015)
- Spahn: schleppende eHealth-Entwicklung, „Todeskampf“ durch Datenschutz (2016)

Bedürfnis nach Vertraulichkeit und Selbstbestimmung

- Fraunhofer SIT, Bürger-Umfrage zu Big Data (2015):
  grundsätzliche Skepsis, Zustimmung bei konkretem Nutzen
- teils begründete Vorsicht im Medizinbetrieb: Sicherung unbefangener Zweitmeinung, Schutz vor Stigmatisierung und Diskriminierung (Risikoselektion)

Neue Ansätze für intelligenteren Datenschutz?

- Gabriel: Datensouveränität statt Datenschutz (Nationaler IT-Gipfel 2015)
- Projektgruppe Smart Data, Positionspapier zum Nationalen IT-Gipfel:
  politischer Handlungsbedarf, konkretere Leitlinien (Anonymisierung, Pseudonymisierung, Zweckbindung)

Privacy nach der DS-GVO

Datenschutz-Grundverordnung der EU (Entwurf)

- Ziel: stärkere Vereinheitlichung des Datenschutzes durch direkt geltende Verordnung
- Politische Einigung im Trilog (Parlament/Rat/Kommission) am 15.12.2015

Weiterer Umsetzungsplan

- formale Verabschiedung in Parlament und Rat noch im 1. Quartal 2016
- Geltung ab 1 . Quartal 2018 (2 Jahre nach Verabschiedung)

Wesentliche Inhalte u.a.

- Geltung auch für Anbieter aus Drittstaaten,
  wenn sie sich an Betroffene in der EU wenden
- verpflichtende Abstimmungsverfahren zwischen den Aufsichtsbehörden
- Erhöhung der Bußgelder auf bis zu 20 Mio. EUR oder
  4 % des weltweiten Jahresumsatzes

Privacy nach der DS-GVO

Zweckbindung (purpose limitation)

- Erhebung nur für bestimmte Zwecke und keine Verarbeitung, die inkompatibel mit diesen Zwecken ist (Art 5 Abs. 1 lit. b)
- zusätzlich muss aber Erlaubnistatbestand vorliegen (Art. 6 ff.)
- Forschung, Statistik und öffentliche Archive i.R.v. Art. 83 Abs. 1 kompatibel

Datensparsamkeit (data minimisation)

- nur die für den Zweck erforderlichen Daten werden verarbeitet (Art 5 Abs. 1 lit. c)

Pseudonymisierung (pseudonymisation)

- Def. in Art. 4 Abs. 3b: keine Zuordnung mehr zu Betroffenem ohne Zusatzinformation
- pseudonyme Daten gelten als personenbezogene Daten (Erw.gr. 23); auch für Dritte, die nicht über die Zusatzinformationen verfügen?
- Art. 6 Abs. 3a lit. 3: Verarbeitung zu anderem Zweck aber eher kompatibel
- soll allgemeine Analysen innerhalb einer verantw. Stelle erlauben, wenn die Zusatzinformation getrennt verwahrt wird (Erw.gr. 23c)
- für sich genommen wohl keine Erlaubnisnorm, jedenfalls nicht für Gesundheitsdaten

Privacy nach der DS-GVO

Besondere Datenkategorien

- darunter genetische, biometrische und **Gesundheitsdaten** (Art. 9 Abs. 1)
- **strengeres Verarbeitungsverbot** (Art. 9 Abs. 1)
- **Ausnahmen** nur nach Art. 9 Abs. 2:

a) ausdrückliche **Einwilligung** für bestimmte Zwecke

b) Erfüllung Pflichten/Ausübung Rechte im Arbeitsverhältnis oder für den Sozialschutz

c) Schutz lebenswichtiger Interessen, wenn Betroffener einwilligungsunfähig

d) interne Verarbeitung von Mitglieder-/Klientendaten bei Non-Profit-Organisationen

e) vom Betroffenen öffentlich zugänglich gemachte Daten

f) Geltendmachung von Rechten / Verteidigung gegen Ansprüche

g) wesentl. öffentliches Interesse a.G. des Rechts der Union oder der Mitgliedstaaten

h) Gesundheitsversorgung aufgrund Gesetz oder Vertrag mit Heilberufler und Berufsgeheimnis nach Abs. 4

hb) öffentliches Interesse im Bereich der **öffentlichen Gesundheit** a.G. Gesetz

i) Forschung, Statistik und öffentliche Archive i.R.v. Art. 83 Abs. 1

Privacy nach der DS-GVO

Art. 83 DS-GVO

- **Archive im öffentlichen Interesse**
- **Forschung** (scientific & historical research)
- **Statistik**
- **Angemessene Garantien** zum Datenschutz in umsetzenden **Rechtsvorschriften**
- insbes. technisch / organisatorisch wie **Datensparsamkeit und Pseudonymisierung**
- **soweit wie möglich ohne Personenbezug**
- Ausnahmen von den Rechten des Betroffenen u.a. auf Auskunft, Korrektur, Sperrung

Privacy nach der DS-GVO

Vorbehalte der Mitgliedstaaten bei Gesundheitsdaten

- einschließlich genetischer und biometrischer Daten (**Art. 9 Abs. 5**)
- Mitgliedstaaten können **weitere Bedingungen, einschließlich Beschränkungen**, in Bezug auf die Verarbeitung dieser Daten beibehalten oder einführen
- **partielle Liberalisierung des Datenschutzes** durch die DS-GVO
  - von der Zweckbindung zur Zweckkompatibilität, insbes. bei Pseudonymisierung
  - evtl. Erleichterung Outsourcing im Gesundheitswesen (Art. 9 Abs. 4)

  müssen **nicht auf Gesundheitsdaten in allen Mitgliedstaaten** übertragen werden
- auch föderale deutsche Datenschutzordnung muss insoweit nicht angepasst werden
- könnte aber weiter harmonisiert werden, aber fraglich, ob es dazu kommt

Föderale Datenschutzordnung in der BRD

Föderale Datenschutzordnung gerade im Gesundheitswesen

- Vielzahl von Regelungen in Bund und Ländern
- erschweren die Bestimmung des jeweils gültigen Regeln

Vorrang des Bundesrechts

- **Sozialgesetzbuch** (SGB V): Kassen, KVen, z.T. Leistungserbringer in der GKV
- **Bundesdatenschutzgesetz** (BDSG) i.Ü. für Arztpraxen, Bundeskliniken, priv. Anbieter
- **Sonderregeln für bestimmte Patientendaten**: GenDG, TPG, AMG (und KFRG)
- **Schweigepflicht** (§ 203 StGB): unbefugtes Offenbaren von Patientengeheimnissen

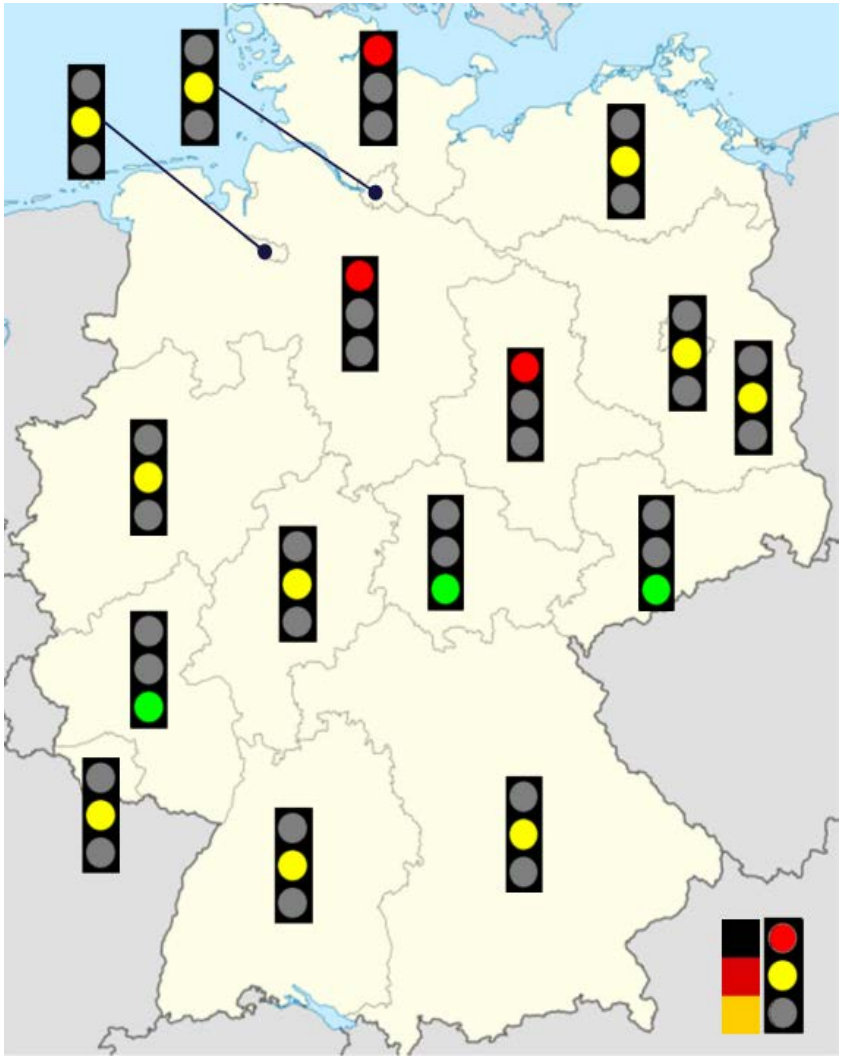
Unterschiedliche Regelungen der Bundesländer

- i.Ü. Gesetzgebungskompetenz bei den Ländern
- **v. a.** für den **Datenschutz** im **Krankenhaus**

Öffnungsklauseln für kirchliche Krankenhäuser

- in Landeskrankenhausgesetzen (LKHG) mancher Bundesländer
- dann gelten für die interne Datenverarbeitung ggf. vorhandene kirchliche Regeln

Beispiel: DV-Erlaubnisse für klinische Qualitätssicherung



Gesetzliche Erlaubnisse für QS:

intern zulässig / extern zulässig
zumindest wenn:
- pseudonymisiert
- ggf. Interessensabwägung

Einschränkungen extern, z.B.:
- Weitergabe nur an bestimmte Personengruppe,
  z.B. ärztlich geleitete Einrichtung
- andere Fachabteilung gilt als Dritter

intern und extern
starke Einschränkungen oder
komplett fehlende gesetzliche Erlaubnis

Grafik: Dr. Astros Chatziastros

Einwilligung (informed consent)

Allgemeine Anforderungen

- **Freiwilligkeit**: kein Zwang, keine Koppelung an (Notfall-)Behandlung
- **Informiertheit**: Aufklärung („informed consent“)
- **Bestimmtheit**: keine Generalermächtigungen
- **Angemessenheit**: bei Formulareinwilligungen (AGB-Kontrolle)
- **Widerruflichkeit**: mit Wirkung für die Zukunft (Ausnahme: klin. Studien nach AMG)

Zusätzlich in einigen Bundesländern für Daten aus Kliniken

- **nicht in allgemeinen Aufnahmebestimmungen** (§ 50 LKHG BW)
- **im Einzelfall** (BW, HB, MV, SL): für konkrete Datenverarbeitung
- **Vorhabensbezug** bei Forschungsvorhaben: Bremen, Saarland
- **nur für krankenhausinterne Forschung** (§ 25 Abs. 1, 2 LKHG Berlin)

Besondere Herausforderung: offenes Data Mining

- **„broad consent“** mit prozeduraler Absicherung über Benachrichtigungspflichten, ...
- **„dynamic consent“** sicherer, jedenfalls wenn Einzelfallbezug gefordert

Anonymisierung & Pseudonymisierung

Anonymisierung vor Smart Data-Verarbeitung

- Zuordnung zu bestimmter / bestimmbarer natürlicher Person (Patient)
- nicht mehr möglich (**absolute Anonymisierung**) oder
- nicht mehr mit verhältnismäßigem Aufwand (**faktische Anonymisierung**)
- für anonyme Daten / Anonymisierung (*strittig*) greift kein Erlaubnisvorbehalt

Pseudonymisierung vor (externer) Smart Data-Verarbeitung

- **Ersetzung** der **Identifikatoren** (Name etc.) durch **Pseudonym**
- um Bestimmung des Betroffenen auszuschließen oder zu erschweren
- Weitergabe Daten ohne die Zuordnung: **kein Übermitteln** v. Patientendaten
- Annahme: Relativität des Personenbezuges (*strittig*)
- **interne Verarbeitung erleichtert** (auch zzt. in DE), aber **Erlaubnisvorbehalt**

Empfehlungen zur Risikovorsorge

- Rest-Risiken der Reidentifizierung bei fakt. Anonymität/ Pseudonymität
- Maßnahmen der **Datensicherheit**
- **Vereinbarungen** mit Datenempfängern: Sicherheit & Reidentifizierungsverbot

Grundlegende Handlungsempfehlungen

1. Klärung des anwendbaren Rechts

- Abhängig von **Art und Sitz der Einrichtung**
- **Art der Gesundheitsdaten** und **Zweck der Verarbeitung**
- Hilfestellung für Forschung und QS: http://irene.tmf-ev.de/homeirene

2. Prüfung der rechtlichen Zulässigkeit

- Ausreichende **Rechtsvorschrift** vorhanden oder
- wirksam die **Einwilligung** des Patienten eingeholt
- oder hinreichende **Anonymisierung** durchgeführt

für QS und Forschung i.d.R. **Pseudonymisierung** notwendige Bedingung – hilfreich: TMF-Leitfaden, vgl. https://www.tmf-ev.de/Produkte/Mustertexte_DSKonzepte2.aspx

3. Gewährleistung der Datensicherheit

- technische und organisatorische Maßnahmen
- **Verschlüsselung** bei Datenübermittlung, differenzierte **Zugriffsrechte** etc.
- vgl. Orientierungshilfe Klinikinformationssysteme (KIS): https://www.datenschutz-bayern.de/technik/orient/oh-kis.pdf

Fazit / Ausblick

Smart Data nach geltendem Recht

- kann grundsätzlich rechtskonform ausgestaltet werden
- allerdings: **Vielzahl von gesetzlichen Regelungen / Restriktionen**
- **Reduktion von Komplexität** über

  Anonymisierung, Pseudonymisierung oder Einwilligung

Denkbare rechtspolitische Ansätze

- **EU-Datenschutz-Grundverordnung**
  - bringt moderate Liberalisierung
  - bzgl. Gesundheitsdaten aber Öffnungsklauseln für Mitgliedstaaten
- **Deutsches Recht**
  - zurückhaltende Nutzung der Öffnungsklausel für Gesundheitsdaten
  - freiwillige Harmonisierung zwischen Bund und Ländern

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Dr. Uwe K. Schneider

Vogel & Partner Rechtsanwälte mbB
Technologiepark Karlsruhe
Emmy-Noether-Straße 17
76131 Karlsruhe

us@vogel-partner.eu
www.vogel-partner.eu