

Datenschutz in der gesetzlichen Krankenversicherung

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz
Schleswig-Holstein
Symposium GKV & Recht 2013
26.09.2013, Berlin

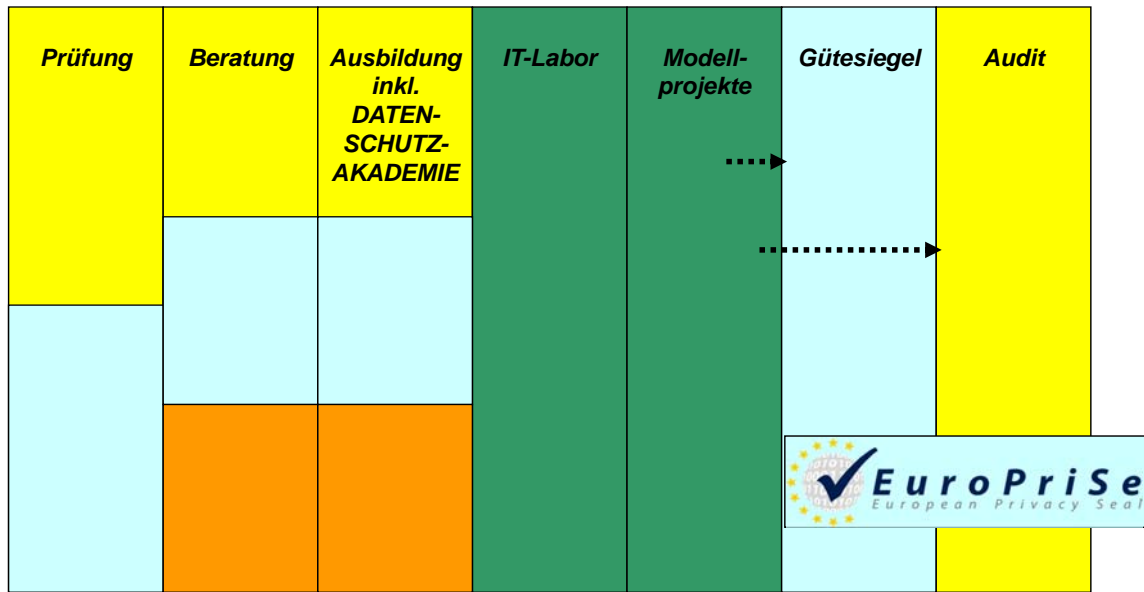


www.datenschutzzentrum.de

Inhalt

- Rechtliche Grundlagen
- Prinzipien des Datenschutzrechtes
- Regelungen des SGB
- Möglichkeiten und Risiken
- Anonymisierung/Pseudonymisierung
- Auftragsdatenverarbeitung - Privatisierung
- Einwilligung
- Elektronische Gesundheitskarte
- Internet

Datenschutz und Informationsfreiheit



Primäre Adressaten:

- Öffentl. Verwaltungen**
- Unternehmen**
- Bürger, Kunden, Patienten**

Wirtschaft, Wissenschaft, Verwaltung

Verfassungsrechtliche Grundlagen

Art. 20 I, 28 I GG Sozialstaatsprinzip

Art. 2 II GG Schutz der Gesundheit

Art. 2 I i.V.m. 1 I GG: allgemeines Persönlichkeitsrecht > Recht auf informationelle Selbstbestimmung, medizinische Selbstbestimmung

Art. 3 GG Gleichbehandlungsgrundsatz, Diskriminierungsverbot

Rechtliche Grundlagen

- Patienten- und Sozialgeheimnis (Eid des Hippokrates, § 203 StGB, Berufsordnungen, § 35 SGB I) > Schutz der Hilfebeziehung
- Wahlfreiheit (u. a. § 76 SGB V)
- Schutz sensibler Daten (§ 3 IX BDSG) > Einwilligung od. gesetzliche Grundlage
- Allgemeines Datenschutzrecht (v.a. BDSG)
- Spezifische Gesetze im Gesundheitsbereich (Krankenhaus-Ge, GesundheitsdienstGe, Forschungsregelungen, KrebsregisterGe, InfSchG ArzneiMG ...)
- > Staatliche Schutz- und Fürsorgepflicht, auch bzgl. Daten
 - > Beschränkung bzgl. Privatisierung

Grundprinzipien des Datenschutzrechtes

- Rechtmäßigkeit
- Einwilligung
- Zweckbindung
- Erforderlichkeit und Datensparsamkeit
- Transparenz und Betroffenenrechte
- Datensicherheit
- Kontrolle

Technisch-organisatorische Schutzziele

- Integrität (Zurechenbarkeit, Unversehrtheit)
- Vertraulichkeit (Unbeobachtetheit)
- Verfügbarkeit (jederzeitige Find- und Nutzbarkeit)
- Transparenz (Revisionssicherheit)
- Intervenierbarkeit (Eingreifbarkeit, Abstreitbarkeit)
- Nichtverkettbarkeit (Zweckbindung, Zwecktrennung, Datensparsamkeit)

Hilfeschutz (besondere Vertraulichkeit)

- Keine Offenbarung möglicher beschämender Notlage (sozial, körperlich, seelisch, familiär, ökonomisch)
- > Tendenziell: Konflikt zu offener Nutzung

Regelungskonzept der Sozialgesetzbücher

Grundnorm: Sozialgeheimnis § 35 SGB I

Allgemeines Datenschutzregelungen: §§ 67 ff. SGB X

GKV: SGB V - Pflegeversicherung: SGB XI

- Kassen, allgm. DV: §§ 284, 288 ff. SGB V, § 94 SGB XI
- Kassen(zahn)ärztliche Vereinigung: § 285 SGB V
- Medizinischer Dienst: §§ 275 ff. SGB V

Sonstige Stellen, z. B.

- Hausarztverbände: §§ 73b, 295a SGB V > BDSG
- Apothekenrechenzentren, § 300 SGB V > BDSG

Gesundheitsspezifische Datennutzung

- Behandlung (incl. Kommunikation, Arbeitsteilung)
- Pflege und Betreuung (incl. Ambient Assisted Living)
- Medizinische Qualitätssicherung u. -kontrolle
- Abrechnung, Versicherung, Wirtschaftlichkeitskontrolle
- Medizinische (u. biotechnologische) Forschung
- (politische, gesellschaftliche) Planung
- Nutzung durch Arbeitgeber
- Wellness und Freizeit, Arbeitsplatz

Risiken

- Beeinträchtigung der Vertraulichkeit (> Inanspruchnahme von Hilfe)
- Beeinträchtigung der Wahlfreiheit
- Medizinische Diskriminierung
- Gesundheitsmanipulation
- Kommerzielle Ausbeutung

Problem bei GKV: Wirtschaftlichkeitsgebot und Wettbewerb
contra Fürsorge- und Solidarprinzip

Anonymisierung/Pseudonymisierung

Regelungen: § 67 Abs. 8, 8a SGB X, § 3 Abs. 6, 6a BDSG

- Ersetzen/Löschen der Identifikatoren (Patient, Arzt, Dienstleister)
- Aggregation (k-anonymity) – abhängig von Quantität, Qualität und Gewichtigkeit der Datensätze

> Anonymität führt zu gewissem Qualitätsverlust

> Pseudonymität ermöglicht Reidentifizierung

bei pseudonymer DV sind Verfahrenssicherungen nötig:
Vertrauensstellen u. Ä.

Beispiele ***Anonymisierung/Pseudonymisierung***

- > Vertragl. Festlegung d. Bewertungsmaßstäbe (§ 87 SGB V)
- > Weitergabe an Apothekenrechenzentren (§ 300 II SGB V)
- > Arzt-Beratungs-Übersicht (§ 305a S. 4 SGB V): 300.000 Einwohner – 1.300 Ärzte
- > Transparenzregeln (§§ 303a ff.)
- > Forschung (§§ 67c V, 75 SGB X, § 98 SGB XI)
- > Risikostrukturausgleich-Weiterentwicklung (§ 268 S. 2-11 SGB V)
- > Qualitätssicherung (§§ 135 ff., 299 SGB V)

Auftragsdatenverarbeitung (§ 80 SGB X, § 197b SGB V)

- Beschränkung auf reine Hilfstätigkeit, keine Funktionsübertragung
- Ultima Ratio (zwecks Vermeidung von „Störungen im Betriebsablauf“ od. „erheblich kostengünstiger“)
- Privilegierung öffentlicher Auftragnehmer
- Nicht überwiegender Teil des Datenbestands
- Präzise Festlegungen zu Gegenstand, Art, Umfang, Dauer, Vorgehen, technische Sicherung, Weisungen, Kontrolle, Löschung
- Mandantentrennung (keine Verwendung für eigene od. fremde Zwecke)
- Aktuelles Problem: Cloud Computing außerhalb Europas

Einwilligung

- Ist grds. zulässig (§ 67 Abs. 2, 3 SGB X)
- Problem Freiwilligkeit (nicht bei Obliegenheit § 60 SGB I)
- BSG, U. v. 10.12.2008 (B 6 KA 37/07 R)): „Eine von den Patienten formularmäßig eingeholte Einwilligungserklärung rechtfertigt die Auftragsdatenverarbeitung nicht. Ein Grundsatz, nach dem unabhängig von einer gesetzlichen Ermächtigung eine Datennutzung und -übermittlung stets zulässig ist, wenn eine Einwilligung – deren Freiwilligkeit in der gegebenen Situation einer Notfallbehandlung zudem fragwürdig ist - vorliegt, greift bei Leistungserbringern nicht“

Beispiele für fragwürdige Einwilligungen

- GKV-Abrechnung durch Krankenhaus (BSG-Fall)
- Früher: Dienstleistereinschaltung bei HzV-Abrechnung
- Krankenfallmanagement
- Selbstauskunft bei Arbeitsunfähigkeit
- Datenkommunikation mit Arbeitgebern
- Generell: unbestimmte Schweigepflichtentbindung
- Werbeeinwilligung in Schulen (auch für befreundete Kassen)

Betroffenenrechte, Transparenz

- Datenschutzrechtliche Betroffenenrechte (§§ 81 ff. SGB X):
Beschwerde bei DS-Aufsicht, Schadenersatz, Auskunft,
Breach Notification, Berichtigung, Löschung, Sperrung,
Widerspruch
- Einschaltung des behördlichen Datenschutzbeauftragten
- Akteneinsicht durch Beteiligte (§ 25 SGB X)
- Versichertenauuskunft/Patientenquittung (§ 305 SGB V)

Medizindatenbeschaffung für Kassen

- Vorlage von Krankenhausentlassungsberichten
 - Vorlage von Reha-Entlassungsberichte
 - Selbstauskunftsbögen für „Beratungszwecke“ (nicht Kontrolle)
 - Indikations- und Begründungsbögen
 - Hausbesuche mit Besuchsprotokolle
- > Medizinische Abrechnungskontrolle erfolgt durch MDK
- > Daten direkt an MDK

Kooperation mit Privaten

- Private Krankenversicherung (§ 194 Ia SGB V)
- Externe Beratungsstellen (24/7, KK-Tarife, Gesundheitsfragen)
- Callcenter
- Hilfsmittellieferanten/-hersteller mit Rabattverträgen

Elektronische Gesundheitskarte (eGK)

- Regelung in §§ 291 ff. SGB V
- Obligatorisch: Berechtigungsnachweis, eRezept
- Fakultativ: Notfalldaten, elektronischer Arztbrief, Arzneimitteltherapiesicherheit, elektronische Patientenakte, Patientenpostfach, Patientenquittung, Organspende, Vorsorgevollmacht/Patientenverfügung
- Doppelter Zugriffsschutz (Arzt-Patient – eGK, PIN, HPC)
- Differenzierte Zugriffsberechtigung
- Protokollierung
- Strenge Zweckbindung (kein Zwang zur Vorlage)

Social Media

Probleme bei sozialen Netzwerken

Selbstorganisation der Mitglieder

- Verantwortlichkeit für Datenverbreitung
- Verarbeitung in den USA
- Trennung Kommunikationsangebot – gesetzliche Aufgaben

Einsatz zur Patienteninformation

Angaben über Versorgung, Tipps, Hinweise

AOK-Ärztenavigator

Einige Schlussfolgerungen

- Bei Einbindung von Privaten verschwimmen klare Grenzen
- Internet ist zumeist keine Lösung
- Telematik-Infrastruktur ist überfällig
- Die DV-Regelungen im SGB V gehören entrümpelt

Datenschutz in der gesetzlichen Krankenversicherung

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-
Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

<https://www.datenschutzzentrum.de>