Datenschutz im Gesundheitswesen - gestern, heute und morgen

Thilo Weichert

Akademische Jubiläumsveranstaltung
60 Jahre Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie - gmds

Mittwoch, 28.10.2015, Köln

Inhalt

- Vertraulichkeit, Stellen, Fragestellungen
- Risiken und Schutzziele
- Datenschutz-Mechanismen
- Anonymisierung/Pseudonymisierung
- Transparenz, Patientenrechte, Auskunftsanspruch
- eGK/Telematik-Infrastruktur
- Europäischer Datenschutz (EU-DSGVO)
- Regulierung u. Regelungsbedarf
- Schlussfolgerungen

Vertraulichkeit und Recht

- Eid des Hippokrates (ärztl. Schweigepflicht, Patientengeheimnis): Vertraulichkeit als Schutz der Hilfebeziehung
- Berufliche Schweigepflicht, § 203 Strafgesetzbuch, Heilberufsordnungen
- Schutz der Gesundheits- und Sozialdaten wegen besonderer Sensibilität (§ 3 IX BDSG, § 35 SGB I, § 67 XII SGB X)
- Schutz in Spezialnormen: KrankenhausGe, GesDG, KrebsRGe, GenDiagnG, InfSchG, TransplG …

> Datenschutz, informationelle und medizinische Selbstbestimmung

Stellen

- Ärzte, Apotheken, Krankenhäuser, Psychologen, Heil- und Pflegedienste
- Informationstechnische Dienstleister (AIS, KIS)
- Netzwerke (Elektronische Gesundheitskarte - eGK, Telematik-Infrastruktur, KV-Safenet, regionale Ärztenetze)
- Abrechnungsstellen (Kassen, KVen, priv. KrankVers., PVS Hausarztverbände, incl. Dienstleister, z. B. ApothekenRZ)
- Kontrollstellen (KVen, MDK, Aufsichtsbehörden, Kammern)
- Forschende, Forschungsnetzwerke, Krankheitsregister
- Wellness-, Lifestyle-Bereich (social media, quantified self)
- Statistik, PharmaU., Werbung, Versicherungen, Arbeitgeber ...

Analysefragestellungen

- Medizinische Behandlung und Betreuung
- Gesundheitsmanagement
- Prävention, Vorsorge
- Pflege (z. B. Ambient Assisted Living)
- Wirtschaftlichkeitskontrolle, Qualitätssicherung
- Biotechnologische und medizinische Forschung
- Selbstoptimierung

Zweckänderung durch

- Versicherungen, Arbeitgeber, Polizei, sonstige Behörden
- Werbung, Pharmavertrieb

Risiken

für PatientInnen/Betroffene

- Beeinträchtigung der Vertraulichkeit
- Beeinträchtigung der Wahlfreiheit
- Medizinische Diskriminierung (z. B. Malus- u. Bonus-Systeme)
- Gesundheitsmanipulation
- Körperliche und seelische Schäden
- Kommerzielle Ausbeutung

für (Gesundheits-) Einrichtung

- Ansehensverlust, Akzeptanzverlust
- Finanzieller Schaden

Materielle Schutzziele

- Privatsphäre
- Vertraulichkeit und Integrität der IT-Systeme / TK-Geheimnis
- Allgemeines Persönlichkeitsrecht
- Hilfeschutz (besondere Vertraulichkeit)

> Keine Offenbarung möglicherweise beschämender (sozialer, körperlicher, seelischer, familiärer, ökonomischer) Notlagen

Technisch-organisatorische Schutzziele

- Vertraulichkeit (z. B. Verschlüsselung)
- Integrität, Authentizität (z. B. Signatur)
- Verfügbarkeit (z. B. Backup, Stromversorgung)
- Intervenierbarkeit (Löschen, Sperren, Korrektur)
- Transparenz, Revisionsfähigkeit (Protokoll, Dokumentation)
- Nichtverkettbarkeit (z. B. Abschottung)

Datenschutz-Mechanismen

- Einwilligung (informed consent): explizit, freiwillig, bestimmt und rückholbar
- Gesetzliche Regelungen

  Materiell:
  Zweckfestlegungen, Daten- und Prozesstransparenz, Verfahrenssicherungen

  Technisch-organisatorisch:
  Verschlüsselung, Pseudonymisierung, Mandantentrennung
- Anonymisierung/Aggregierung

Anonymisierung/ Pseudonymisierung

- Löschen od. Ersetzen der Identifikatoren durch Pseudonyme (bzgl. Patient, Arzt, Abrechner, Dienstleister)
- Aggregierung von Datensätzen u./o. von Merkmalsdaten

Instrumente

- Krankheitsregister (z. B. Krebs) mit Treuhänder
- Datentransparenz unter staatlicher Aufsicht und Kontrolle (z. B. §§ 303a ff. SGB V)
- Mehrschichtige Pseudonymisierungsverfahren (z. B. Biobanken, Problem: potenziell unbeschränktes Zusatzwissen, z. B. aus dem Internet)

Transparenz

Adressaten:

- Betroffener (auch Recht auf Nichtwissen)
- Heilberuf (Arzt, Krankenhaus …)
- (staatliche) Aufsicht, Verwaltungshierarchie
- Demokratisch legitimierte und rechtliche Genehmigungs- und Kontrollinstanzen (z. B. DS-Aufsicht, Ethik-Kommissionen)
- (wissenschaftliche) Fachöffentlichkeit
- Öffentlichkeit

Patientenrechte

Grds. „Informed Consent“ (medizinisch u. informationell)

- Recht auf Auskunft und Einsicht
- Recht auf Information und Benachrichtigung
- Recht auf Löschung und Gegenvorstellung (Widerspruch, Sperrung, Berichtigung)
- Recht auf Schadenersatz
- Recht auf externe Kontrolle (bDSB, DS-Aufsicht, Kammer, Ombudsmann, Verbraucherzentralen, Gerichte)

Technische Unterstützung bei Wahrnehmung der Patientenrechte (eKiosk, Internet)

Elektronische Gesundheitskarte eGK rechtlich

- Wenige Pflichtanwendungen (Identifikation, Stammdatenabgleich)
- Freiwillige Funktionen (Notfalldaten, Arztbrief, Pat. Akte, Patientenfach, Organspende, Pat.verfüg.)
- Transparenz und Information für Versicherte
- Sicherung der Einwilligung
- Differenzierter Datenzugriff
- Schutz vor mittelbarem Zwang

eGK – Telematikinfrastruktur techn.

- Integrität und Authentizität (HPC, dig. Signatur)
- Datenverfügbarkeit (Backup)
- Vertraulichkeit (elektron. Verschlüsselung, diff. Berechtigungsvergabe)
- Revisionssicherheit (Protokollierung)
- Medizinorientierung (IT als Unterstützung, nutzerfreundliche Oberfläche)
- Patientenorientierung (Kioske, Postfachlösung, evtl. Internet-Schnittstellen)

Europäische Datenschutz-Grundverordnung (EU-DSGVO)

Ablauf

- 12/2012 EU-Kommission
- 4/2014 EU-Parlament
- 6/2015 EU-Rat, jetzt Trilog

Inhalte

- Harmonisierung, One-Stop-Shop, Kohärenzverfahren
- u. a. Einwilligung, besondere Datenkategorien, Statistik, Forschung ...

Europäische Datenschutz-Grundverordnung

Art. 81 – Verarbeitung für Gesundheitszwecke

- Grundlage Unionsrecht od. Mitgliedstaatsrecht„ das geeignete, besondere Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht“

Zwecke:

- Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Ges. Versorgung, Behandlung, Verwaltung von Gesundheitsdiensten, wenn ärztl. oder ähnl. Personal mit Geheimhaltungspflicht tätig wird
- Gründe des öffentlichen Interesses für Gesundheit, hohe Qualitäts- u. Sicherheitsstandards f. Arzneimittel u. Med.Pr
- Andere Gründe öffentlichen Interesses: soziale Sicherheit, Qualität, Wirtschaftlichkeit und Abrechnung von Kr.Versicherung

Art. 81 EU-DSGVO

- Bzgl. Geschichte, Statistik + Forschung Verweis auf Art. 83, Ergänzung Parlament: Anonymisierung od. wenn nötig Pseudonymisierung „gemäß den höchsten technischen

Standards“ > Verhinderung der Reidentifizierung

- Kommission: Delegierte Rechtsakte durch Kommission bzgl. „Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“ + „Kriterien und Anforderungen in Bezug auf die Garantien“, Parlament: Stellungnahme von Europäischem Datenschutzausschuss ist nötig
- Parlament neu: Mitgliedstaaten müssen Vorschriften melden, Art. 82a: Soziale Sicherheit „durch ihre öffentlichen Einrichtungen“ + Meldepflicht

Art. 83: u. a. Forschung, Statistik

- Zweckerreichung auf andere Weise nicht möglich
- Filetrennung Stammdaten – Merkmalsdaten
- Veröffentlichung grds. nur bei Einwilligung
- Parlament: bes. Schutz bes. Datenkategorien, Ausnahme von Einwilligung nur bei „außergewöhnlich großem öffentlichen Interesse“
- Rat: Weite Erforderlichkeitsregelung, wenn „angemessene Garantien“, Konkretisierung durch nationales Recht

Nationale Regelungen

- E-Health-Gesetz (BT-Drs. 18/5792), 1. Lesung im Bundestag Juli 2015 > Einführung eGK, Arztbrief, konsiliarische Behandlung …, Öffnung der Telematik-Infrastruktur
- Einschaltung IT-Dienstleister mit zusätzlichem Schutz (Beschlagnahme, Berufsgeheimnis) ?
- Ungeklärt: Outsourcing Abrechnung, Handel mit pseudonymen Patientendaten

Weiterer Regelungsbedarf

- Abbau des Regelungswirrwarrs (Bund, Land - Krankheitsbezug, Adressatbezug)
- Bessere Absicherung von Betroffenenrechten
- Patientenvertretung
- Zertifizierung und Standardisierung
- Big Data im Gesundheitswesen (z. B. für Forschungszwecke)

Weitere Regelungsformen

Konkretisierungen des BDSG bzw. der EU-DSGVO

- Selbstregulierung (Kammern, Branchen, Forschungsgemeinschaften)
- Best Practice, SOPs
- Verhaltensregeln

Schlussfolgerungen

für die Betroffenen

- Daten sind nicht Informationen
- Computer können nicht behandeln, sondern nur unterstützen
- Vertraulichkeit ist nicht obsolet

gesamtgesellschaftlich

- Stärkung des IT- und Gesundheitsstandorts
- Verbesserung der Gesundheit
- Stärkung der individuellen Selbstbestimmung
- Gesundheitsservice als staatliches Angebot (Private-Public-Partnership

Datenschutz im Gesundheitswesen - gestern, heute und morgen

Thilo Weichert

Waisenhofstr. 41, 24103 Kiel

0431 9719742

thilo.weichert@t-online.de