Digitale Medizin und Datenschutz

Dr. Thilo Weichert, Leiter des ULD

22. vfa-Round-Table

mit Patienten-Selbsthilfegruppen

Digitale Medizin – Chance für Patienten?!

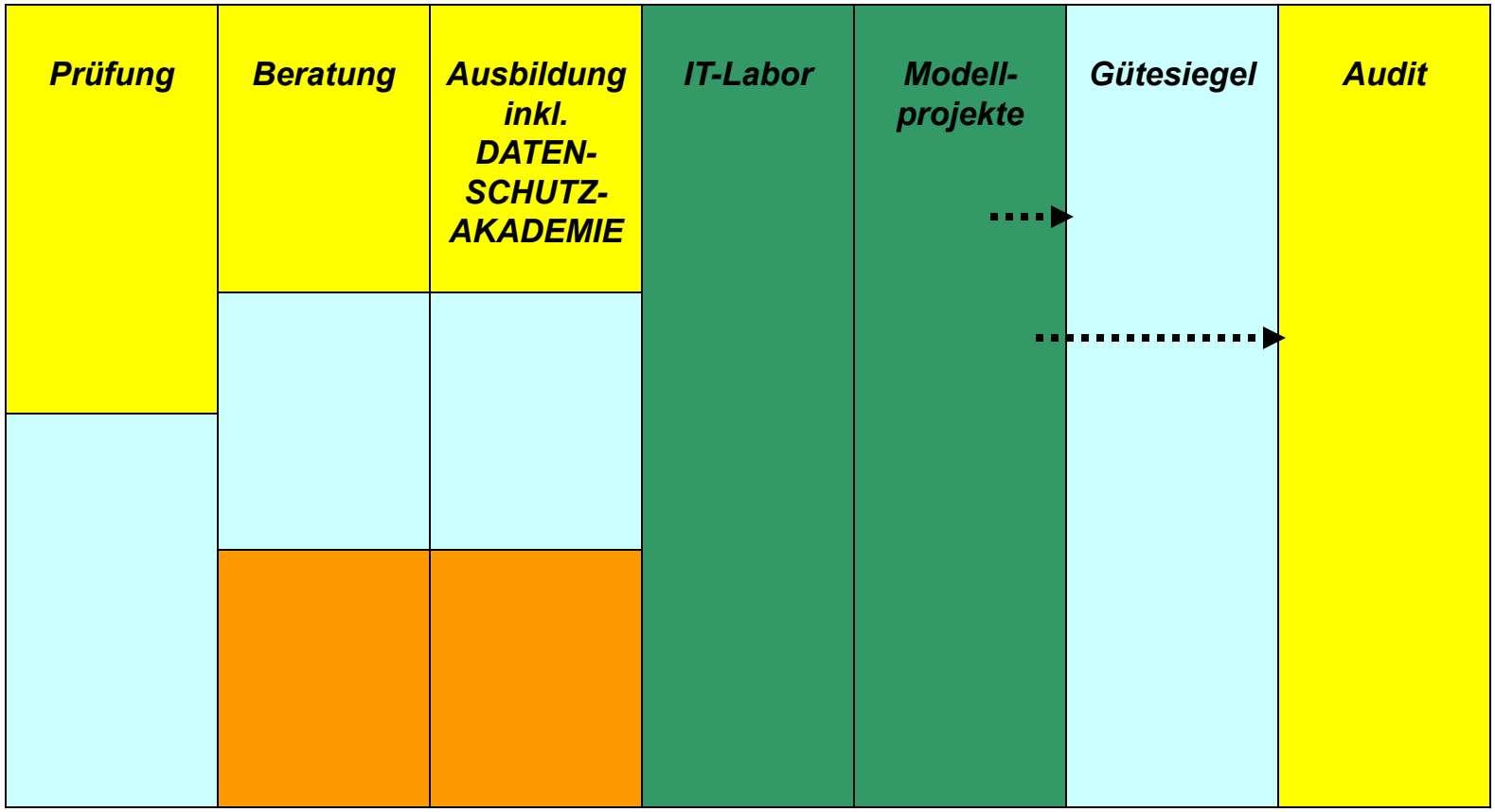
Berlin, 26. Juni 2015

Inhalt

- Unabhängiges Landeszentrum für Datenschutz
- Vertraulichkeit, Stellen, Fragestellungen
- Risiken und Schutzziele
- Datenschutz-Mechanismen
- Anonymisierung/Pseudonymisierung
- Transparenz, Patientenrechte, Auskunftsanspruch
- eGK/Telematik-Infrastruktur
- Europäische Datenschutz-Regulierung
- Regelungsbedarf
- Schlussfolgerungen

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Datenanalyse bei Health Care

Die 3+1 Vs von Big Data

- Volume
- Variety
- Velocity

> Value

Versprechen

- Kostenersparnis
- Medizinische Erkenntnis
- Prävention und personalisierte Behandlung
- Daten für effektive Planung und Organisation

> Qualitätsverbesserung + Goldgrube

Vertraulichkeit und Recht

- Eid des Hippokrates (ärztliche Schweigepflicht, Patientengeheimnis): Anvertrauen als Schutz des für Hilfe notwendigen Vertrauensverhältnisses
- Berufliche Schweigepflicht § 203 Strafgesetzbuch, Heilberufsordnungen
- Schutz der Gesundheitsdaten wegen besonderer Sensibilität (§§ 3 IX BDSG, 67 XII SGB X)
- Schutz durch Spezialnormen: KrankenhausGe, GesDG, KrebsRG, GenDiagnG, InfSchG, AMG, TransplantG …
- > Datenschutz, informationelle und medizinische Selbstbestimmung

Verarbeitende Stellen

- Ärzte, Apotheken, Krankenhäuser, Psychologen, Heil- und Pflegedienste
- Informationstechnische Dienstleister (AIS, KIS)
- Elektronische Gesundheitskarte (Telematik-Infrastruktur)
- Abrechnungsdaten (Kassen, KVen, priv. Krankenversicherungen, Hausarztverbände, incl. Dienstleister z.B. ApoRZ)
- Qualitätssicherung und Wirtschaftlichkeitskontrolle
- Gesundheitsforschung (Forschungsnetzwerke, Krebsregister)
- Wellness-, Lifestyle-Bereich (social media, quantified self)
- Statistik, Werbung, Versicherungen, Arbeitgeber …

Analyse-Fragestellungen

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

Stark zweckändernde Bedarfe:

- Versicherungen
- Arbeitgeber
- Polizei und Behörden

Risiken

Für Patienten/Betroffenen

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

Für (Gesundheits-) Einrichtung

- Ansehensverlust, Akzeptanzverlust für bes. Maßnahmen
- Finanzielle Schäden

Schutzziele

Datenschutz

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Intervenierbarkeit
- Transparenz
- Nichtverkettbarkeit

Hilfeschutz (besondere Vertraulichkeit)

- Keine Offenbarung möglicher beschämender Notlage (sozial, körperlich, seelisch, familiär, ökonomisch)

> Tendenziell: Konflikt zur offenen Nutzung

Datenschutz-Mechanismen

- Einwilligung (informed consent) muss explizit, freiwillig, bestimmt (wer, was, wofür) und rückholbar sein

- Gesetzliche Regelungen

  materiell: Zweckfestlegungen, Information, Erklärung

  technisch-organisatorische Vorkehrungen (Verschlüsselung, Psedonymverarbeitung)

  Verfahrenssicherungen (Genehmigungen u. Ä.)

- Anonymisierung/Aggregierung

Anonymisierung/Pseudonymisierung

- Löschung od. Ersetzen der Identifikatoren durch Pseudonyme (bzgl. Patient, Arzt, Abrechner, Dienstleister)
- Aggregierung der Merkmalsdaten

Lösungen:

- Krankenheitsregister (z. B. Krebs) mit Treuhänder
- Forschungsgeheimnis u. qualifizierte Einwilligung
- Datentransparenz unter staatlicher Aufsicht und Kontrolle (§§ 303a SGB V)
- Mehrschichtige Pseudonymisierungsverfahren (Problem: unendliches Zusatzwissen)

Transparenz

Adressaten (mit differenziertem Informationszugang):

- Betroffener (auch Recht auf Nichtwissen),
- Arzt, Krankenhaus, Heilberuf (evtl. als Treuhänder)
- (staatliche) Aufsicht, Verwaltungs-Hierarchie
- Demokratisch legitimierte und rechtliche Genehmigungs- und Kontrollinstanzen (z. B. DS-Aufsicht, Ethik-Kommission)
- (wissenschaftliche) Fachöffentlichkeit
- Öffentlichkeit

Patientenrechte

Generell: informed consent (medizinisch und informationell)

- Recht auf Auskunft und Einsicht
- Recht auf Information und Benachrichtigung
- Recht auf Löschung und Gegenvorstellung (bzw. Widerspruch, Berichtigung)
- Recht auf Schadenersatz
- Anrufung bDSB, Ärztekammer, Ombudsmann, Datenschutzaufsicht, Verbraucherzentralen

technische Unterstützung bei Wahrnehmung der Patientenrechte (eKiosk, Internet)

Auskunftsanspruch

Grundlage

- Behandlungsvertrag
- Medizinische Selbstbestimmung
- Informationelle Selbstbestimmung

Inhalt

- Konkrete Daten, Herkunft, verarbeitende Stellen, Zweck

auch zu pseudonymer Datenverarbeitung

evtl. digital erschlossen (elektronische Patientenakte)

eGK – Selbstbestimmung contra Fremdbestimmung

- Funktionalität, Autonomie und Diskretion contra Manipulations- u. Diskriminierungsgefahr u. Kontrolle
- Verpflichtende Anwendungen: Identifikation, Abrechnung, elektronisches Rezept (?)
- Freiwillige Anwendungen: Notfall- bzw. Basisdaten, elektronischer Arztbrief, Arzneimitteldokumentation, elektronische Patientenakte, Patientendokumente, Organspende

§ 291a Sozialgesetzbuch V

- Nutzung nur für Inanspruchnahme von (zahn-) ärztl. Leitungen (§ 291 I 2)
- Definierte Datenfelder (§ 291 II)
- Sicherung der Transparenz (§ 291a i.V.m. § 6c BDSG)
- Information der Versicherten (§ 291 III 2)
- Sicherung der Einwilligung (§ 291a III 4)
- Differenzierter Datenzugriff (§ 291a IV, V)
- Schutz vor mittelbarem Zwang (§ 291a VIII)

Generelle Anforderungen an Telematik-Infrastruktur

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

Europäische Datenschutz-Regulierung

Vorschlag Europäische Datenschutz-Grundverordnung (EU-DSGVO)

Entwurf EU-Kommission 12/2012

Beschluss EU-Parlament (1. Lesung) 12.03.2014

Stellungnahme EU-Rat 6/2015, jetzt: Trilog

- One-Stop-Shop für Unternehmen in Europa
- Europaweite verbindliche materielle Regelungen
- Kohärenzverfahren der (unabhängigen) Aufsichtsbehörden, Europäischer Datenschutzausschuss
- Effektiver Rechtsschutz für Betroffene (vor nationalen Gerichten)

Art. 81 EU-DSGVO I

- 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
- 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.Versich.

Art. 81 EU-DSGVO II

- 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

Nationale Regelungen bleiben relevant

- Aktuell: E-Health-Gesetz – Umsetzung der eGK/Telematik-Infrastruktur > E-Entlass-Brief, E-Arzt-Brief, E-Konsultation
- Bald?: Ausnahmeregelung für IT-Dienstleistungen für Berufsgeheimnisträger (Besondere Verpflichtung und Auswahl, strenge Erforderlichkeit, technische Sicherungen)
- Viele weitere brennende ungelöste Datenschutzfragen: Outsourcing Abrechnung, Handel mit pseudonymisierten Patientendaten

Regelungsbedarf

- Abbau des Regelungswirrwarrs (Bund, Land – Krankheitsbezug, Adressatbezug)
- DV-Befugnis für IT-Dienstleisterbefugnis
- Bessere Absicherung von Betroffenenrechten, Patientenvertretung
- Zertifizierung und Standardisierung

- Per Selbstregulierung (Kammern, Branchen, Forschungsgemeinschaften) Best Practice, SOPs, Verhaltensregeln
- Konkretisierung der Europäischen Datenschutzgrundverordnung
- Fortschreibung des SGB V

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
- IT-Gesundheitsservice als staatliches Angebot (Private-Public-Partnership)

Digitale Medizin und Datenschutz

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

https://www.datenschutzzentrum.de