Sicherheitsaspekte der elektronischen Gesundheitskarte

Dr. Thilo Weichert, Leiter des ULD

IT-Sicherheit am Donaustrand
Kultur- und IT-Speicher Regensburg
7. Juli 2010

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Vorstellung des ULD
- Medizinische und informationelle Selbstbestimmung: Vertraulichkeit und Wahlfreiheit
- Zwecke und Interessen
- Generelle Anforderungen an eGK-Medizintelematik als IT-Großprojekt
- § 291a Sozialgesetzbuch V
- Technische Sicherungen
- Rollen – politische Konflikte
- Best Practice – Audit – Gütesiegel
- Perspektiven

Vorstellung des ULD

Datenschutzbehörde in Schleswig-Holstein

- Kontrolliert Patientengeheimnis und Medizindatenschutz im öffentlichen und nicht-öffentlichen Bereich
- Berät PatientInnen und (Zahn-) ÄrztInnen – u.a. auch über die Aktion „Datenschutz in meiner Arztpraxis“ https://www.datenschutzzentrum.de/medizin/arztprax/index.htm
- Führt Forschungsprojekte durch, z.B. Datenschutz bei Biobanken od. bei Ambient Assisted Living
- Bietet Auditverfahren und Datenschutz-Gütesiegel an (u.a. European Privacy Seal – EuroPriSe)
- Berät Beteiligte beim eGK-Pilotprojekt Flensburg

Grundlagen

Medizin bei Hippokrates (400 v.Chr.) und im 21. Jahrhundert

- Arbeitsteilung > Datenaustausch
- IT-Einsatz > komplexe Nutz- und Auswertbarkeit der Daten

Individualrechtl. Schutz durch Verfassung (Grundgesetz - GG)

- Art. 2 Abs. 2 GG: Schutz der Gesundheit
- Art. 12 GG: Schutz der Berufsfreiheit
- Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: Schutz der Rechte auf „informationelle Selbstbestimmung“ und „Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen“

Vertraulichkeit und Wahlfreiheit

Volkszählungsurteil des BVerfG 1983: „Jede Person hat das Recht selbst zu bestimmen, wer was wann bei welcher Gelegenheit über sie weiß“

- Gesetzesvorbehalt oder Einwilligung
- Vorrang der Datenerhebung beim Betroffenen
- Zweckbindung
- Grundrechtsschutz durch Verfahren

BVerfG 1999: Der Patient hat grds. „einen Anspruch auf Einsicht in die ihn betreffenden Krankenunterlagen“

Wahlfreiheit als Konkretisierung des Rechts auf
medizinische u. informationelle Selbstbestimmung
(vgl. § 76 SGB V: Freie Arztwahl)

Spezifizierter Individualgrundrechtsschutz

- Wissen und Bestimmen über pers.bez. Datenverarbeitung
- bestimmte gesetzliche, verhältnismäßige Eingriffsgrundlage
- Technische, organisatorische und prozedurale Schutzvorkehrungen

➢ Verbot von Persönlichkeitsprofilen
➢ Verbot der Rundumüberwachung
➢ Verbot der anlasslosen Kontrolle („ins Blaue hinein“)
➢ Schutz des Kernbereichs persönlicher Lebensgestaltung
➢ Systemschutz (Integrität, Vertraulichkeit, Authentizität, Verfügbarkeit, Revisionssicherheit, Transparenz, Unverknüpfbarkeit)

Selbstbestimmung als Gemeinschaftsgut

Bundesverfassungsgericht:

Recht auf informationelle Selbstbestimmung (Datenschutz)

„Selbstbestimmung ist eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“.

Patientengeheimnis (ärztliche Schweigepflicht)

Der Schutz des Patientengeheimnisses „dient, im Ganzen gesehen, der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge“

Zwecke des IT-Einsatzes

- Optimierung der Behandlung
  bessere Information, bessere Kommunikation, Verhinderung von Doppeluntersuchungen
- Verbesserung der Selbstbestimmung der PatientInnen

- Optimierung der Abrechnung
- Rationalisierung und Kostenersparnis
- Wirtschaftlichkeits- und Qualitätskontrolle
- medizinische u. pharmazeutische Forschung und Entwicklung
- Patientendaten haben wirtschaftlichen „Wert“

> Konfliktpotenzial für Wahlfreiheit und Patientengeheimnis

(Zahn-) Ärztliche Interessen

Contra IT-Einsatz

- Zusätzliche IT-Investitionen
- Zusätzlich nötiges IT-Know-how
- Verstärkte Gefahr für Patientengeheimnis
- Entpersönlichung des (Zahn-) Arzt-Patientenverhältnisses

Pro IT-Einsatz

- Mehr und bessere, schnell verfügbare Medizininformationen
- Erleichterte Arbeitsteilung
- Qualifiziertere Behandlung
- Rationalisierung der Praxisabläufe
- Technische Sicherung von Patientendaten
- Verbesserung der Patientenautonomie

Generelle Anforderungen an Medizintelematik

- 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)

Anforderungen an IT-Großprojekte

- Kein Zeitdruck (Gesetz: 2006, Wirklichkeit ?)
- Einbeziehung von allen Beteiligten/Betroffenen bei Planung und Durchführung
- Vermittlung von hinreichender Medienkompetenz
- Stufenförmiges Vorgehen: Planung, Erprobung, Freigabe, Evaluation, Modifikation (organisches Wachstum)
  - Forschung und Entwicklung
  - Organisation
  - Erprobung und Test (Modellprojekte, Flächenerprobung)
  - Freigabe und Inbetriebnahme
  - dauernde Evaluation und Pflege (Systemmanagement)
- Modulares Vorgehen bei verschiedenen Funktionalitäten

eGK – Selbstbestimmung contra Fremdbestimmung

- Autonomie und Diskretion contra
  Manipulation und Kontrolle (ohnmächtiger Patient)
- Verpflichtende Anwendungen: Identifikation, Abrechnung, (elektronisches Rezept)
- Freiwillige Anwendungen: Notfall- bzw. Basisdaten, elektronischer Arztbrief, Arzneimitteldokumentation, elektronische Patientenakte, Patientendokumente

§ 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)

Technische Sicherungen I

- Individuell verschlüsselte Ablage (zentral oder dezentral)
- Grds. doppelte Nutzungsautorisierung (Patient, Arzt)
- Authentisierung durch digitale Signatur (HPC, SMC)
- Kombination von Karten- (z.B. Basis- bzw. Notfalldaten, eRezept) und Netzspeicherung (z.B. elektronische Patientenakte, eRezept)
- Kommunikation über Virtual Private Network (VPN), keine oder nur beschränkte Schnittstellen zum Internet
- Weitere technisch-organisatorische Maßnahmen (§ 9 BDSG)

Technische Sicherungen II

- Genügen die vorgesehenen Datensätze den Prinzipien der Erforderlichkeit und Datensparsamkeit?
- Sind die Daten während der Speicherung und bei Übermittlungen vor unberechtigtem Zugriff ausreichend geschützt?
- Gewährleistet das Zugriffskonzept, dass Lese- und Schreibberechtigungen nur im Rahmen des Erforderlichen und vom Patienten Gewollten eingeräumt werden?
- Wird der Urheber jedes Datums eindeutig identifiziert und protokolliert?
- Ist gewährleistet, dass die Systemadministration keinen Zugriff auf patientenbezogene Daten erhält?
- Wird der mindestens 10jährigen Dokumentationspflicht genügt?
- Können Daten gelöscht und/oder gesperrt werden?
- Kann die Auskunftserteilung an die PatientInnen problemlos erfolgen?
- Sind die Wahlrechte der PatientInnen technisch abgebildet?
- Ist die Anwenderoberfläche so gestaltet, dass (Zahn-) Ärzte und Patienten die Kontrolle über die automatisierten Vorgänge behalten?

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 (Kiosk, Internet)

Funktionalität contra Sicherheit

- Fehlendes Systemverständnis contra Komplexität der Einwilligung
- Stapelanwendungen contra differenzierte Wahl
- Multimorbidität contra Eingabe der sechsstelligen PIN (keine Default-/Komfort-PIN)
- Basis(Notfall)datenverfügbarkeit contra Vertraulichkeit
- Freie Arztwahl contra ärztliche Treuhänderschaft
- Begrenzter Internet-Zugang (PIN@home) contra VPN
- Backup bei Kartenverlust contra Missbrauchsrisiko

> Technische Modifikation konventioneller Abläufen

Rollen I

PatientInnen

- Mehr Information, Wahlmöglichkeit und Verantwortung
- Hauptinteresse Gesundheit, nicht Autonomie
- Objekt der DV > Treuhänderregeln bei technisch ohnmächtigen, „unmündigen“ od. behinderten Patienten

(Zahn-) ÄrztInnen

- Erhöhte IT- und Datenverantwortlichkeit (incl. Datentreuhänder)
- Verstärkte Lotsenfunktion

Rollen II

Gematik, Staat

- System- und Netzverantwortlichkeit (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)

Verfasste (Zahn-) Ärzteschaft

- Prozessbegleitung
- Interessenwahrung für Ärzteschaft und PatientInnen
- Information der Öffentlichkeit

Politische Konflikte

- Gewinner (Kassen, Gesundheitsverwaltung, IT-Branche, spezialisierte und technisierte Medizinanbieter)
  contra Verlierer (Hausarzt, Apotheke um die Ecke, konventionelle Medizin)
- Parteipolitik (FDP/Linke contra SPD/CDU)
- Wer trägt die Kosten – wer macht Gewinne?
- Modernisierung & Globalisierung contra Patientenorientierung
- Instrumentalisierung des Datenschutzes (gläserner Patient, gläserner Arzt, zentrale Speicherung)

Best Practice - Audit - Gütesiegel

- Hilfen für Best Practice durch Verbände, Kammern, Datenschutzaufsichts- und Datensicherheitsbehörden
- Etablierung von Datenschutzmanagementsystemen
  Vorabkontrolle je Modul
  Regelwerk technisch, organisatorisch (Abläufe), rechtlich
  Einbeziehung von Leitung, Admin. bDSB, Anwendende
- Datenschutz-Gütesiegel für IT-Produkte
- Datenschutz-Audit für Einrichtungen und Verfahren

Perspektiven

Es kommt darauf an, gemeinsam die Vertraulichkeit des Gesundheitswesens aus der Zeit des Hippokrates in unsere Informationsgesellschaft hinüberzuretten.

Sicherheitsaspekte der elektronischen Gesundheitskarte

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de