Vertraulichkeitsschutz durch IT-Sicherheit bei der elektronischen Gesundheitskarte

9. Deutscher IT-Sicherheitskongress
10.-12. Mai 2005 - Bonn - Bad Godesberg
Bundesamt für Sicherheit in der Informationstechnik

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
(ULD)

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Übersicht

- kein Zeitdruck
- IT-Verfahren in einer freiheitlichen Demokratie
- mahnende Beispiele
- Vertraulichkeit medizinischer Behandlung
- Datenschutz bei der elektronischen Gesundheitskarte (eGK)
- Rolle der Patientinnen und Patienten
- Herausforderungen an die Sicherheitstechnik
- Patientenfreundliche Implementation der eGK
- Schlussfolgerungen

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Kein Zeitdruck

Zeitdruck bringt Projekt voran

Feste Termine sind für erfolgreichen Projektabschluss Gift

- Einführung von Technologie lässt sich nicht verordnen
- technisch: modulare Entwicklung nötig
- sozial: Akzeptanz der Bevölkerung geboten
- kulturell: Ausbildung am System

das braucht Zeit und Geld

IT-Verfahren in einer freiheitlichen Demokratie

Demokratie bedingt einen ergebnisoffenen öffentlichen Diskurs

Sicherung der Transparenz von Verfahren und Verwaltung

Wahrung der Grundrechte auf Berufsfreiheit und Eigentum

Förderung der Informationsfreiheit

Wahrung des Rechts auf informationelle Selbstbestimmung

Mahnende Beispiele

Bundesweite IT-Großprojekte mit planungsbedingten Hindernissen:

- LKW-Maut-System
- Banken-Kontoevidenzverfahren
- JobCard-Verfahren
- A2LL - Arbeitslosengeld II
- biometrische Ausweisdokumente

Anforderungen neben Funktionalität und Wirtschaftlichkeit:

Datenschutz und Transparenz

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Vertraulichkeit medizinischer Behandlung I

Konstituierende Voraussetzung für medizinische Selbstbestimmung und leistungsfähige Gesundheitsfürsorge

Herausforderungen am Patientengeheimnis à la Hippokrates

- Arbeitsteilung
- Einsatz von Informations- und Biotechnologie

Zwecke moderner Datenauswertungen:

- Abrechnung, Wirtschaftlichkeits- und Qualitätskontrolle
- Weiterentwicklung von Diagnostik, Behandlung, Medikation
- Forschung
- informationelle/medizinische Selbstbestimmung

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Vertraulichkeit medizinischer Behandlung II

Funktionale Herausforderung durch Kommunikation und Vernetzung in umfassendem Telematikkonzept:

- Rezeptierung
- Medikationskontrolle
- Notfalldatenvorhaltung
- Behandlungsdokumentation
- Patientendatenverwaltung

Inhaltliche Herausforderung:

- Autonomie
- Diskretion

für Arzt und Patient

Datenschutz bei der elektronischen Gesundheitskarte

§§ 291, 291a SGB V bilden Datenschutz (Patientengeheimnis/Transparenz/Wahlfreiheit) rechtlich ab

Patient bleibt schwächstes Glied bei Patientendatenverarbeitung
wegen Abhängigkeit von Krankheit
wegen fehlender rechtlicher u. technischer Kompetenz

> Technikgestaltung ist von zentraler Bedeutung
rechtliche Vorgaben sind systemtechnisch umzusetzen

Rolle des Patienten

- Patient ist faktisch Objekt nicht Subjekt der Datenverarbeitung
- Patient hat subjektive Rechte: Bestimmung Datenempfänger (Einwilligung), Auskunft/Akteneinsicht, evtl. Gegendarstellung
- Patient hat keinen Einfluss auf Dokumentation, Systemauswahl, Netznutzung, Datensicherheit (Behandlungshintergrund)

ökonomische Interessen als Gefahren für Patienten

– Ärzte/Krankenhäuser/Apotheken: Profit, zumind. Kostendeckung
– Krankenkassen: Kostenminimierung
– IT-Anbieter: Markterschließung
– Pharmaindustrie: Patientenbindung, Medik.-Monitoring

zentraler Anküpfungspunkt für Wahrung d. Patientenrechte:

– Freiwilligkeit der Anwendungen
– Nichtnutzung der vertrauensunwürdigen Anwendungen

Herausforderungen an die Sicherheitstechnik

Bewältigung der komplexen Struktur in Hinblick auf
- Funktionalität der Anwendungen
- gesicherte Verantwortlichkeiten
- Wahrung von Vertraulichkeit und Wahlmöglichkeit

– Erforderlichkeit u. Datensparsamkeit
– Schutz vor unberechtigtem Zugriff (Verschlüsselung Pseudonymisierung)
– differenziertes Zugriffs- und Rollenkonzept
– Dokumentauthentifizierung und Nutzungsprotokollierung
– Abschottung vor Systemadministration
– Sicherung der Dokumentationspflicht und der Korrekturansprüche
– Sicherung der Patiententransparenz (Auskunft, Belegverfahren)
– Abbildung der Wahlrechte
– Anwenderfreundlichkeit (Ärzte- und Patientenschaft)

Patientenfreundliche Implementation der eGK I

als rechtliche, soziale, kulturelle, organisatorische und politische Aufgabe

für Ministerien, Kassen, Softwarehäuser, Berufsverbände, Datenschützer und dort v.a. auch Techniker

zentrale Rahmenbedingungen:

- modularer Entwicklungsprozess
- Transparenz
- unabhängige Auditierung
- Vermittlung von Medienkompetenz

Patientenfreundliche Implementation der eGK II

modularer Entwicklungsprozess

- mehrstufige Einführung bzgl. Anwendungen
- Korrekturfähigkeit von Entwicklung über Implementierung bis Betrieb
- Berücksichtigung weicher und harter Faktoren

Transparenz

- Entscheidungs- und Implementierungsverfahren
- konkrete Datenverarbeitung
- keine security by obscurity, für offene Standards

unabhängige Auditierung (Datenschutz u. Datensicherheit)

- Gütesiegel für eingesetzte Produkte
- Auditierung ganzer Anwendungen/Verfahren

Vermittlung von Medienkompetenz

- kostenträchtige Ausbildung von Ärzten und Patienten

Schlussfolgerungen

- Vertrauen ist ein Zustand und ein Prozess
- Vertraulichkeit ist die Herausforderung für die IT-Sicherheitstechnik
- eGK kann zum Vorzeigeprojekt für bürgerfreundliche IT-Großverfahren werden
- Der Weg in die Informationsgesellschaft ohne die Betroffenen ist eine Sackgasse

Vertraulichkeitsschutz durch IT-Sicherheit bei der elektronischen Gesundheitskarte

Dr. Thilo Weichert

Wo?	Unabhängiges Landeszentrum für Datenschutz 24103 Kiel, Holstenstraße 98
Telefon?	0431/988-1200
Telefax?	0431/988-1223
E-Mail?	weichert@datenschutzzentrum.de
Internet?	www.datenschutzzentrum.de/
der Vortrag?	www.datenschutzzentrum.de/vortraege/

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN