

# Datenschutz und Datensicherheit im Umfeld klinischer Anwendungen

Reinhard Vetter

Bayerischer Landesbeauftragter für den  
Datenschutz

# Agenda I

## insb.rechtliche Rahmenbedingungen

- n Arztgeheimnis und Datenschutz
- n Patientenrechte
- n DV - Voraussetzungen
- n Zugriffsrechte auf DV - Systeme im Krankenhaus
  - u Grundlagen
  - u Zugriffsrechte im einzelnen
  - u Organisatorisch - technische Umsetzung
- n Elektronische Gesundheitskarte und -  
Patientenakte

# Arztgeheimnis und Datenschutz

## n Arztgeheimnis

- u Schweigepflicht - auch gegenüber nicht behandelnden Ärzten - es sei denn:
- u Einwilligung oder spezielle gesetzl. Befugnis

## n Datenschutz

- u Recht, über DV selbst zu entscheiden
  - F Eingriffe nur im überwiegenden Interesse der Allgemeinheit auf gesetzlicher Grundlage
- u Recht auf Datensicherheit

# Patientenrechte

- n Freie Arztwahl
- n Einverständnis zur Behandlung
- n Einverständnis zur Datenverarbeitung
- n Auskunfts- und Informationsrechte
- n Recht auf sichere Datenverarbeitung

# DV-Voraussetzungen

## n Datenverarbeitung muß berechtigt sein

### u Einwilligung, Behandlungsvertrag

- F informiert
- F freiwillig
- F i.d.R. schriftlich
- F schlüssiges Handeln, mutmaßliche Einw.

### u Gesetzliche Befugnisse u.a.

- F Art. 27 BayKrG
- F SGB V

### u Güter- und Interessenabwägung

## n Technik schafft keine Befugnisse

# Zugriffsrechte auf DV-Systeme im Krankenhaus - Grundlagen

- n keine beliebige Offenbarung von Patientendaten
- n Schweigepflicht auch zw. Krankenhausärzten
- n Art. 27 IV 1 BayKrG: Nutzung von Patientendaten durch Krankenhausärzte
- n Art. 27 IV 2 BayKrG: durch die Verwaltung
- n Erforderlichkeit: Objektive Eignung zur Zweckerreichung und Angemessenheit

# Nutzung von Patientendaten durch Krankenhausärzte

“Die Krankenhausärzte dürfen Patientendaten nutzen, soweit dies im Rahmen des krankenhausesärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist”.

# Nutzung von Patientendaten durch die Verwaltung

“Die Krankenhausverwaltung darf Patientendaten nutzen, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich ist”

# Folgerungen für Zugriffsrechte

- n Behandelnde Fachabteilung: Alle Daten
- n Freigabe für mit- oder nachbehandelnde Abt. soweit erforderlich durch Eintrag im System
  - u kein Selbsteintrag
  - u Information und Einwilligung des Patienten
  - u Genehmigung von Ausnahmeregelungen durch Klinikvorstand (z.B. bei Geburtshilfe oder Kinderkliniken)
- n Alle Fachabteilungen: Reduzierter Datensatz
- n Baldmögliche Anonymisierung bei Zugriff zu Forschungszwecken

# Benutzerverwaltung, Berechtigungen

- n Ziel: Zugriff nur auf Daten, die für die Aufgabenerfüllung benötigt werden
- n Differenzierte Zugriffsrechte, Berechtigungskonzept
- n Personenbezogene Benutzerkennungen
- n Eindeutige Identifikation und Authentifikation der Benutzer
- n Schneller Benutzerwechsel am Arbeitsplatz

# Patientenkarte

## § 291 a SGB V - § 97 Abs. 2 StPO

- n Pflichtteil - freiwilliger Teil
  - u Keine informationelle Vermischung mit Pflichtkarte
  - u Freiwilligkeit für medizinische Daten allgemein und im Einzelfall, besonderes Patientenfach - § 291 a Abs. 3
  - u Datentransparenz durch Lese- und Kontrollrechte - § 291 a Abs. 4 u. 6
- n Gewährleistung von Beschlagnahmeschutz und Zeugnisverweigerungsrecht - § 97 Abs. 2 StPO
- n Sanktionierung des Fehlgebrauchs, z.B. bei Arbeitgebern oder Versicherung - § 307, 307 a SGB V

# Elektronische Patientenakte

- n Gewahrsam des Arztes
- n Einwilligung in Datenspeicherung und Abruf für den jeweiligen Behandlungsfall
- n Besondere Einwilligung für sensible Facharztbereiche
- n kein Zugriff für nichtbehandelnde Ärzte
- n kein zentraler Datenpool

# Agenda II

technisch - organisatorische Ziele und Anforderungen an  
klinische Informationssysteme

- n Benutzerverwaltung, Berechtigungen
- n Grundlegende Sicherheitsziele
- n Protokollierung, Fernwartung
- n Weitere Maßnahmen
- n Digitale Archivierung

# Grundlegende technisch-organisatorische Sicherheitsziele

- n Integrität
- n Authentizität
- n Verfügbarkeit
- n Vertraulichkeit
- n Revisionsfähigkeit

# Protokollierung

- n Ziel: Nachvollziehbarkeit der Datenverarbeitung
- n Änderungen der Benutzerverwaltung und an Patientendaten
- n Fehlversuche bei der Benutzeranmeldung
- n Externe Datenübertragungen
- n Regelmäßige Auswertung der Protokolle, keine Verhaltens- und Leistungskontrolle

# Fernwartung

- n Ziel: Keine Kenntnisnahme der Daten durch die Wartungsfirma nach Möglichkeit
- n Bei Arbeiten am Echtsystem:
  - u Verbindungsaufbau unter Kontrolle des Klinikums - call back Verfahren
  - u Protokollierung aller Aktionen
  - u Verschlüsselte Datenübertragung
  - u Mitverfolgung am Bildschirm, Abbruchmöglichkeit
  - u Änderung des Passworts nach jeder Fernwartung
  - u Verpflichtung Externer auf das Datengeheimnis

# Weitere Maßnahmen zur Sicherheit der Patientendaten

- n Sperrung von Daten entlassener Patienten
- n Elektronische Signatur, Unveränderbarkeit von Daten, Historie der Datenänderungen
- n Verschlüsselte Datenübertragung und -speicherung bei unsicheren Umgebungen
- n Absicherung der Außenanbindungen, z.B. Firewall

# Digitale Archivierung

## Grundsätzliches

- n Ziel: Dauerhafte Auslagerung von Daten aus dem sofort zugreifbaren Datenbestand
- n Sichere Aufbewahrung und Registrierung der Speichermedien, räumliche Zugangskontrolle
- n Nicht - Überschreibbarkeit der Daten
- n Auslesen/Wiedereinspielen der Daten nur durch Berechtigte und im Bedarfsfall
- n keine Datenkenntnis beim Provider

# Verschlüsselte Datenspeicherung im Archiv

- n Verschlüsselung mit ausreichender Schlüssellänge nur im Krankenhaus
- n Bereitstellung von Verfahren zur eventuellen Umschlüsselung
- n Erfüllung der üblichen Anforderungen an die Rechenzentrumssicherheit

# Weitere Anforderungen

- n Gesicherte Einsatzumgebung im Klinikum
  - u Sicherheitsmaßnahmen beim Einscannen von Altakten
  - u Sichere Installation und Initialisierung des Archivierungssystems
  - u Sichere Aufbewahrung der Schlüssel
  - u Gesicherte Anbindung an den Provider
- n Organisatorische Maßnahmen Provider
  - u Personelle Trennung unterschiedlicher Aufgaben
  - u Verpflichtung der Mitarbeiter
- n Beachtung der Grundsätze der Auftrags - DV

# Weitere Informationen

- n Patientenverwaltungssysteme :  
<http://www.datenschutz-bayern.de/technik/orient/patdatkh.html>
- n Verschlüsselte Datenarchivierung bei externen Providern: <http://www.datenschutz-bayern.de/tbs/tb21/k22.html#22.2.3.2>
- n Fernwartung: <http://www.datenschutz-bayern.de/tbs/tb18/k3.html#3.3.4>