

# Datenschutz und Datensicherheit in Gesundheitsanwendungen

## Praktischer Datenschutz

Manfred Brunner (Erlangen)

GMDS-AG „Datenschutz in Gesundheitsinformationssystemen (DGI)“

---



# Praktischer Datenschutz

## Anforderungen und Konzepte



# Beauftragter für den Datenschutz Anspruch und Wirklichkeit (1)

- Verpflichtende schriftliche Bestellung in Krankenhäusern (mehr als 4 Mitarbeiter)
  - *Wird meist erst nach Androhung von Bußgeld umgesetzt*
- Anforderungen:
  - Fachkunde
    - *Dem Beauftragten ist Gelegenheit zu geben, Kenntnisse zu erwerben*
      - *Juristische Fachkenntnisse*
      - *Informationstechnologie*
      - *Betriebswirtschaft*
      - *Organisation*
      - *Schulung*



# Beauftragter für den Datenschutz Anspruch und Wirklichkeit (2)

- Zuverlässigkeit
  - *Persönliche Integrität*
  - *Keine Interessenskonflikte*
    - *Weitere Aufgaben, die mit der Funktion im Widerspruch bzw. Spannungsverhältnis stehen (Geschäftsleitung, Leiter Personalabteilung, Aufgaben die der Beauftragte kontrollieren soll)*
- Auswahlprinzipien
  - *der junge, der sich nicht wehren kann*
  - *der alte, den man abschiebt*
  - *der ungeliebte streitbare*
  - *der kompetente, der den Laden kennt*



# Beauftragter für den Datenschutz Anspruch und Wirklichkeit (3)

- Stellung
  - Unmittelbar dem Leiter unterstellt
  - Weisungsfrei auf dem Gebiet des Datenschutzes
  - Keine Benachteiligung wegen der Erfüllung seiner Aufgaben
    - *Oftmals ist Zivilcourage erforderlich*
- Verpflichtung
  - Verschwiegenheit über
    - Identität von Betroffenen
    - Hinweise auf Betroffene



# Beauftragter für den Datenschutz Anspruch und Wirklichkeit (4)

- Unterstützung durch den Dienstherrn bei Erfüllung der Aufgaben
  - Hilfspersonal
    - *Wird kaum umgesetzt*
  - Räume
  - Einrichtungen
    - *Die Minimalausstattung*
  - Geräte und Mittel
    - *Welche Mittel? Ein eigener Etat!*
- *Zusammenarbeit mit IT-Sicherheitsexperten ist nötig. Aufbau einer eigenen Infrastruktur.*
- Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden



# Beauftragter für den Datenschutz - Aufgaben Anspruch und Wirklichkeit (1)

- Er wirkt auf die Einhaltung des Datenschutzgesetzes und anderer Vorschriften über den Datenschutz hin
  - Grundgesetz
    - Art. 1. Die Würde des Menschen ist unantastbar
    - Art. 2. Recht auf freie Entfaltung der Persönlichkeit
    - Recht auf informationelle Selbstbestimmung
  - Bundesdatenschutzgesetz
  - Europäische Datenschutzrichtlinie
  - Ärztliche Schweigepflicht



# Beauftragter für den Datenschutz - Aufgaben Anspruch und Wirklichkeit (2)

- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
  - Voraussetzung: rechtzeitige Unterrichtung
  - *Eine gewaltige Aufgabe: wie kontrolliert man denn eine Anwendung, ob sie ordnungsgemäß ist?*
- Schulungen
  - Vertrautmachen der Mitarbeiter mit den Vorschriften über den Datenschutz sowie mit den jeweiligen Erfordernissen des Datenschutzes



# Beauftragter für den Datenschutz - Aufgaben Anspruch und Wirklichkeit (3)

- Verfahrensverzeichnis
  - Verantwortlicher für das Verzeichnis
  - Der Dienstherr liefert die Daten
    - *Der Beauftragte muß sie sich nicht holen!*
- Vorabkontrolle (Verfahrensfreigabe)
  - Beurteilung der Verfahren
    - *Bei komplexen Softwaresystemen sind erhebliche Kenntnisse erforderlich*
    - *IT-Sicherheitskenntnisse sind erforderlich*
    - *Eine Beurteilung erfordert auch Kenntnis des Leistungskatalogs*
    - *Checklisten sind ungeeignet*



# Praktischer Datenschutz

## Beispiele und gelebte Praxis



# Grundsätze

- Wahrung der ärztlichen Schweigepflicht
  - Der Behandlungszusammenhang ist unumstößliche Vorgabe
- Need-to-know-Prinzip
  - Mitarbeiter sollen nur Zugriff auf die von ihnen benötigten Daten haben
- Technische und organisatorische Maßnahmen treffen zum Schutz der Patientendaten
  - Verhältnismäßigkeit wahren
  - Verwendung kryptographischer Verfahren
- Datenschutz soll nicht behindern, sondern als Gewinn betrachtet werden.



# Benutzerverwaltung und Zugriffsberechtigungen im KIS (1)

- Grundsätzlich darf in einem KIS jeder Benutzer nur auf die Daten zugreifen, die er für seine Aufgabenerledigung benötigt.
  - Eigene geheime Kennung
  - Definierte detaillierte Rechte
    - Datensätze – Untermengen – Datenfelder
  - Zugriffsart
    - Lesen, Schreiben
- Problem:
  - Dauer von An- und Abmelden
  - Kartenbasierte Authentisierung besser als Benutzername und Passwort
    - HPC, Transponder, Biometrische Merkmale



# Benutzerverwaltung und Zugriffsberechtigungen im KIS (2)

- Benutzer- und Aufgabenbezogenes Berechtigungskonzept
  - Rollenkonzept, das auf der Organisationsstruktur des Krankenhauses basiert
    - Arzt, Pfleger, Verwaltung, ...
  - Notfallkennung
  - Anonymisierung für Unberechtigte
    - Labor
  - Mitarbeiter als Patient, VIPs
    - *Anonymisierung, rechtmäßig?*
  - Notfalldaten
    - *Hoffnung auf die eGK*



# Benutzerverwaltung und Zugriffsberechtigungen im KIS (3)

- Probleme:
  - Anzahl der Rollen
  - Pflege der Berechtigungen
  - Rollenwechsel
  - Automatisches Feststellen des Behandlungszusammenhangs
- *Wünschenswert wäre die automatische Zugriffsrechtevergabe durch Erkennung des Behandlungszusammenhangs ausgehend vom gespeicherten Datum selbst*



# Fernwartung (1)

- Zugriff auf personenbezogenen Daten durch die Wartungsfirma soll verhindert werden
- Lösungsvorschlag 1:
  - Testsystem ohne Personenbezug
  - *Selten möglich*
- Lösungsvorschlag 2:
  - Anonymisierung der Daten
  - *Großer Aufwand bei einem Datenvolumen von vielen GB und mehreren 10000 Personenbezügen*



## Fernwartung (2)

- Vorgeschlagenes Prozedere (Bayerischer Landesbeauftragter) bei unvermeidbarem Zugriff durch externe Firmen:
  - Verbindungsaufbau auf Veranlassung und unter Kontrolle des Anwenders
  - Protokollierung aller Aktionen
  - Vertraulichkeit der Daten bei der Übertragung sicherstellen (Verschlüsselung)
  - Ständige Kontrolle am Bildschirm (Abbruchmöglichkeit)
  - Änderung des Passworts für den Fernwartungszugang nach jeder Nutzung



## Fernwartung (3)

- Probleme:
  - Personalaufwand
  - Proaktive Wartung
    - *Nur möglich bei kontinuierlichem Zugang*
  - Fernwartung außerhalb der Dienstzeit:
    - *Oft gewünscht, um Betriebsstörungen zu minimieren*
    - *Arbeitszeitregelung*



# Telemedizin (1)

- Zusammenarbeit mit externen Partnern
  - Integrierte Versorgung
    - Datenaustausch über E-Mail
    - Anbindung an das KIS
  - Dienstleistung
    - Tele-Konsile
    - Tele-OP, Tele-Anästhesie, ...
  - Kooperation
    - Hosting von Krankenunterlagen
  - Elektronische Patientenakte



# Telemedizin (2)

- Technische Anbindung
  - E-Mail Versand
    - Sicherstellung von Integrität, Vertraulichkeit, Authentizität und Nichtabstreitbarkeit der Datenübermittlung
    - Verschlüsselung
    - revisionsfeste Protokollierung
  - Anbindung an das KIS
    - Schutzmaßnahmen gegen unbefugten Zugriff auf personenbezogene Daten
    - Firewall, Intrusion Detection Systeme
    - Verschlüsselung



## Telemedizin (3)

- Speicherung von Krankenunterlagen im Krankenhaus
  - Gefordert durch verschiedene landesweite Krankenhausgesetze
  - als Dienstleistung des Krankenhauses
  - Erweiterung der Benutzerverwaltung und des Berechtigungskonzepts
    - Schreibender und lesender Zugriff des externen Arztes
- Speicherung bei einem externen Provider
  - Beschlagnahmeschutz gewährleistet
  - Empfehlenswert:
    - Trennung des Personenbezugs
    - Personenbezugsherstellung beim Arzt



## Telemedizin (4)

- Erfahrungen:
  - Ärztliche Praxen sind auf einem technologisch schlechten Stand
  - Das Datenschutzbewußtsein beim niedergelassenen Arzt ist nicht sehr ausgeprägt
  - Die technische Betreuung sollte nicht dem Arzt überlassen werden
  - Praxiscomputer sollten restriktiv in Ihre Internetfähigkeit eingeschränkt werden.
  - Schulungen sind notwendig



# Protokollierung (1)

- Überprüfung der Rechtmäßigkeit von Zugriffen
  - Wer hat wann welche Daten verarbeitet?
- Benutzung des Notfallzugriffs
- Revisionsfähigkeit (vorgeschrieben)
  - Benutzer mit Zugriffsrechten und Historie müssen ebenfalls protokolliert werden
    - Wer hat wann welche Berechtigungen besessen?
- Fernwartung
  - Verbindungsaufbau, Dauer
  - Zugriffe auf welche Daten



# Protokollierung (2)

- Probleme:
  - Lesbare Protokolle
    - Ein Dump ist nicht lesbar!
    - Übersichtlichkeit
    - Nur der benötigte Inhalt darf enthalten sein
  - Wer führt das Protokoll?
    - Ist den Fremdfirmen zu trauen?
  - Kann das Protokoll automatisch ausgewertet werden?



## Zukünftige Anforderungen – eGK, HBA (2007, 2008, 2009 ...?)

- Die eGK ist eine weitere Schnittstelle mit dem Patienten
- Aufklärung der Patienten (wer macht das?)
- Die Einwilligung verlangt Informiertheit
- Regelung der Vertretung des Patienten
- eGK-Nutzung durch Patienten
  - Nutzung der Rechte
- Zugriffsberechtigung für Fachgruppen



# Ausblick

- Datenschutz und IT-Sicherheit müssen als unterschiedliche Bereiche angesehen werden und können auch nicht von einer Person repräsentiert werden.
- Der Datenschutzbeauftragte wird in Zukunft sein Amt ohne Unterstützung von IT-Sicherheitsexperten nur eingeschränkt wahrnehmen können.
- Aber:
  - So lange nichts passiert, geschieht auch nichts!

