Datenschutz · Ergonomie · Mitbestimmung
www.sovt.de

Erstellung eines Datenschutzkonzepts für ein Krankenhausinformationssystem

Probleme, Erfahrungen, Lösungsansatz

Heide, 17. Mai 2001

Lothar Bräutigam
(Dipl. inform.)

Herdweg 10a
64285 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Wer ist sovt?

- **Beratung zum betrieblichen Datenschutz**
  - Schwerpunkt: Datenschutz im Krankenhaus
  - Schwerpunkt: Arbeitnehmerdatenschutz
  - Entwicklung eines Datenschutzleitfadens für Siemens medico//s
  - Externer Datenschutzbeauftragter
  - Seminare zum betrieblichen Datenschutz
- **IT- und Organisationsberatung**
  - Ergonomieberatung, Gefährdungs-analysen, Software-Ergonomie
  - Beratung & Seminare für Betriebs- und Personalräte

Herdweg 10a
64285 Darmstadt

Tel. (06151) 62 60 2
Fax (06151) 62 60 6
eMail: info@sovt.de
Internet: www.sovt.de

Überblick

1. **Einführung, Problemlage**
2. Anforderungen des Datenschutzes im Krankenhaus
3. Praxisfälle – Härtetest für ein Krankenhaus-Informationssystem
4. Datenschutz im Krankenhaus umsetzen: Wie vorgehen?
5. Diskussion

Herdweg 10a
64285 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Datenschutz im Krankenhaus

- Krankenhaus-Informationssysteme nicht mehr wegzudenken
- Weitere Ausweitung der Funktionalität, z.B.
  - DRGs
  - Pflegedokumentation
  - Elektronische Patientenakte (Imaging)
  - Internet-Anbindung
- Einsatz überspannt (fast) alle Bereiche im Krankenhaus

➔ **Immer mehr personenbezogene Daten!**

Und der Datenschutz?

Probleme des Datenschutzes im KH

- Rasante Entwicklung der Technik und Ausweitung Ihres Einsatzes
- Zu geringe Personalkapazitäten
- Kostendruck
- Datenschutz keine strategische Aufgabe, kein Wettbewerbsvorteil
- Hersteller von KIS liefern mangelhafte Datenschutztechnik
- Datenschutz wird bei KIS-Projekten häufig nicht ernst genommen
- Datenschutz wird nicht als organisatorische Aufgabe aufgefasst

Lösung?

Der Datenschutz ist so umzusetzen, dass

- ein flexibler Umgang mit den Patientendaten ermöglicht wird,
- die Arbeitsprozesse im Krankenhaus nicht behindert werden,
- die hohen Anforderungen an den Datenschutz und die ärztliche Schweigepflicht trotzdem umgesetzt werden,
- die praktikabel ist und nicht am perfektionistischen Anspruch scheitert.

Heilung und Lebensrettung haben Vorrang, aber:

Aufgabe anderer Grundrechte

(z.B. Recht auf informationelle Selbstbestimmung)

Überblick

1. Einführung, Problemlage
2. **Anforderungen des Datenschutzes im Krankenhaus**
3. Praxisfälle – Härtetest für ein Krankenhaus-Informationssystem
4. Datenschutz im Krankenhaus umsetzen: Wie vorgehen?
5. Diskussion

Herdweg 10a
64285 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Recht auf informationelle Selbstbestimmung

Auch im Krankenhaus:

Das Recht auf informationelle Selbstbestimmung erfordert den Schutz des einzelnen vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Es umfasst **„die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“**

- Abgeleitet aus allgemeinem Persönlichkeitsrecht, VZ-Urteil des BVerfG, 1983
- Das Recht auf informationelle Selbstbestimmung kann nur durch eine **präzise gesetzliche Grundlage** eingeschränkt werden, z.B. Datenschutzgesetze, Sozialgesetzbuch, Krankenhausgesetze.

Zulässigkeit der Verarbeitung

ERLAUBNIS
zur Verarbeitung personenbezogener Daten

durch Rechtsvorschrift

- **andere Rechtsvorschrift**
  (bereichsspezifischer Datenschutz)
  - Landeskrankenhausgesetz
  - Ärztliche Schweigepflicht
  - Bes. Vorschriften zur Übermittlung:
    → §§ 73 (1b), 275 ff., 295, 301 SGB V
    → § 100 (1) SGB X, § 202 SGB VII
    → § 22 (3) BPflV
- **BDSG bzw. LDSG**
  - Erforderlichkeit
  - Zweckbindung
  - Bes. Vorschriften zur Verarbeitung von Gesundheitsdaten

durch Einwilligung des Betroffenen

Grundsatz:

Verbot mit Erlaubnisvorbehalt

(§ 4 Abs. 1 BDSG)

Zulässigkeit der Verarbeitung

§ 45 LKG-BW:

Zulässigkeit der Erhebung, Speicherung, Veränderung und Nutzung

- Zur Versorgung des Patienten
- Zur Dokumentation der Versorgung
- Zur verwaltungsmäßige Abwicklung der Behandlung

Sofern nicht anonymisiert möglich und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen:

- Zur Qualitätssicherung
- Zur Wahrnehmung von Aufsichts- und Kontrollpflichten, zur Rechnungsprüfung, ...
- (...)

Beispielkrankenhaus in Baden-Württemberg, kommunaler Eigenbetrieb

Zulässigkeit der Verarbeitung

Zulässigkeit der Übermittlung ⇢ *gilt für Übermittlungen an Personen und Stellen außerhalb des Krankenhauses*

- § 46 LKG-BW
- **Ärztliche Schweigepflicht** ⇢ *gilt auch gegenüber anderen Ärzten, auch innerhalb des Krankenhauses*
  (Ärztliche Berufsordnung i.V.m. § 203 StGB)
- Andere Rechtsvorschrift
- Einwilligung des Patienten

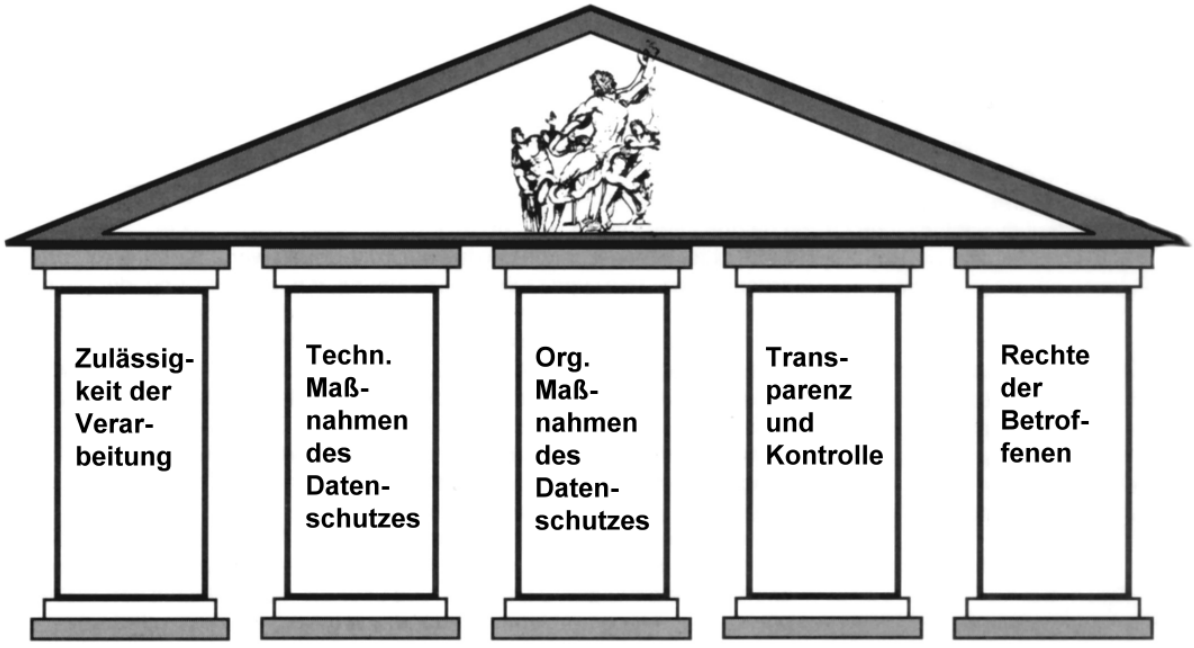
↓

Abschottung der Fachabteilungen untereinander sowie von der Verwaltung

↓

Zugriffsberechtigungen

Weitere Anforderungen des Datenschutzes



Überblick

1. Einführung, Problemlage
2. Anforderungen des Datenschutzes im Krankenhaus
3. **Praxisfälle – Härtetest für ein Krankenhaus-Informationssystem**
4. Datenschutz im Krankenhaus umsetzen: Wie vorgehen?
5. Diskussion

Herdweg 10a
64285 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Praxisfälle

Welche Zugriffsrechte für ...

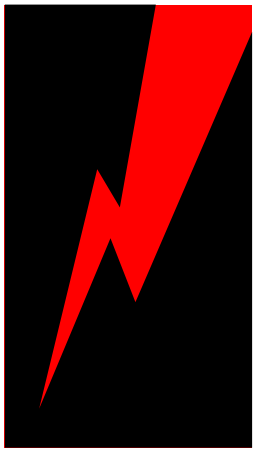
... Konsiliarärzte?
... Notfälle, für Vertretungszwecke, für Springer?
... Funktionsbereiche?
... die Pflegedienstleitung?
... Controlling?
... Systemadministratoren, Datenschutzbeauftragte?

Gelten die Zugriffsrechte bis ...

... Behandlungsende?
... zur Abrechnung?
... zur nächsten Aufnahme?
... zur Löschung der Daten?

Anforderungen an KIS

- Differenziertes, einheitliches Zugriffsschutzsystem
- Situationsbezogene, individuelle Freischaltungen und Entzug von Zugriffsberechtigungen
  - Konsil, Verlegung, Entlassung (Abrechnung), ...
- Geeignete, schnelle Authentisierungsverfahren
- Detaillierte, flexibel definierbare Protokollierung
  - nicht nur „Eingabekontrolle“, auch Auswertungen
  - auch Systemverwaltungsaktivitäten, Fernwartung
- Anonymisierung bzw. Pseudonymisierung von Patientendaten
  - z.B. für Controlling-Auswertungen
- Sperren und Löschen von Patientendaten
  - Sperren von Patientendaten nach der Entlassung
  - Definition und automatisierte Umsetzung von Löschfristen
- Verschlüsselungstechniken



Datenschutz · Ergonomie · Mitbestimmung

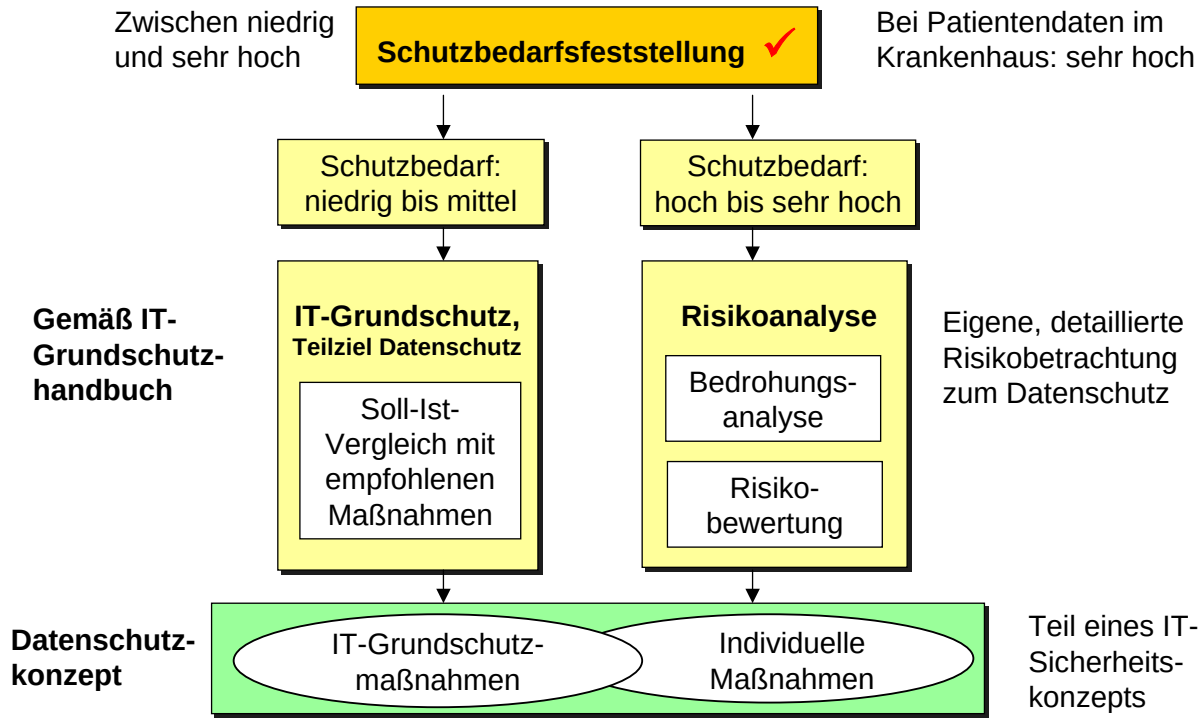
www.sovt.de

Überblick

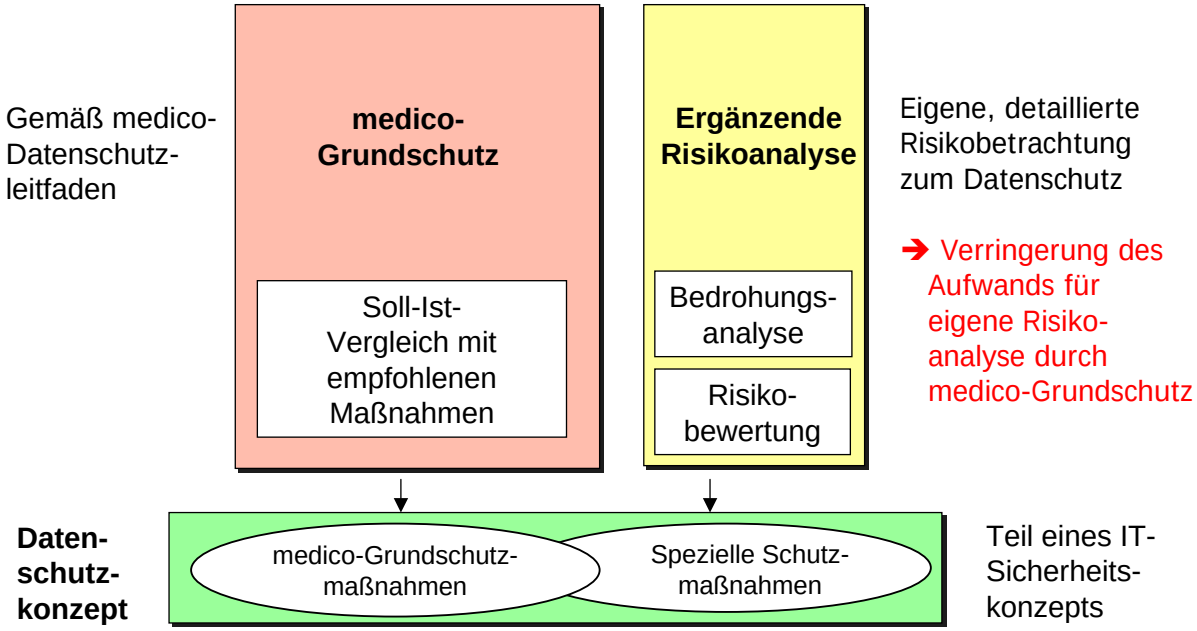
1. Einführung, Problemlage
2. Anforderungen des Datenschutzes im Krankenhaus
3. Praxisfälle – Härtetest für ein Krankenhaus-Informationssystem
4. **Datenschutz im Krankenhaus umsetzen: Wie vorgehen?**
5. Diskussion

Herdweg 10a
64285 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Erstellung eines Datenschutzkonzepts



Erstellung eines Datenschutzkonzepts



Organisatorische Umsetzung

- Einrichtung einer Projektgruppe zur Planung und Umsetzung des Datenschutzkonzepts
  - Beteiligung aller für den Datenschutz wichtigen Personen und Organisationseinheiten
  - Festlegung von Aufgaben, Kompetenzen, Budgets, Terminen etc.
- Effektives Projektmanagement
  - Geeigneter Projektleiter
  - Methodeneinsatz
  - Verbindlichkeit
- Unterstützung durch die Krankenhausleitung

Medico-Datenschutzleitfaden

1. Anforderungen des Datenschutzes an den Betrieb eines KIS
2. Vorgehensweise zur Erstellung eines Datenschutzkonzepts
3. Gefährdungen beim Betrieb eines KIS
4. Katalog technischer, organisatorischer und personeller Maßnahmen zum Datenschutz
5. Checkliste zur Anwendung des Datenschutz-Leitfadens

Anhang: Datenschutz-Ordner

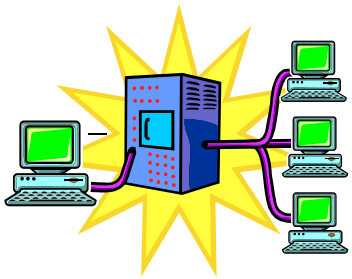
Zusätzlich für Auftraggeber:

Anforderungen des Datenschutzes an die weitere Software-Entwicklung

Methodische Unterstützung

Datenschutz-Ordner

- zur konkreten Handlungsanleitung (Strukturierung und Hilfen)
- für ein effektives und effizientes Vorgehen
- zur strukturierten Dokumentation der Ergebnisse (Datenschutzhandbuch)



Geeignetere Form:

➔ **Intranet-Anwendung**

Methodische Unterstützung

Vortrag „Erstellung eines Datenschutzkonzepts für ein KIS“

Inhalt des Datenschutzordners:

- Allgemeine Angaben zum Verfahren (Zweckbestimmung, Rechtsgrundlagen)
- Rechtsvorschriften
- Konfiguration (Hardware, Software, Netzwerk)
- Personenbezogene Daten
- Zugriffsberechtigte Personen (primär stellenbezogen)

Bestandsaufnahme

- Risikoanalyse (Bedrohungen analysieren und bewerten)

Risikoanalyse

- Technische und organisatorische Maßnahmen des Datenschutzes
- Dienstanweisung
- Unterrichtung der Beschäftigten (Qualifizierungsplanung)

Datenschutz-konzept

- Verfahrensverzeichnis
- Vorabkontrolle

Gesetzliche Dokumentationspflichten

Empfehlungen

- Die Hersteller vertraglich auf die Umsetzung des Datenschutzes verpflichten
- Datenschutz projektbegleitend bearbeiten
- Methodengeleitetes Vorgehen
- Intelligente Ersatzlösungen für fehlende technische Datenschutzmaßnahmen
- Datenschutz umsetzen ist auch Organisationsentwicklung
- Verantwortlichkeiten zum Datenschutz verbindlich klären (Dienstanweisung zum Datenschutz)
- Wichtig: Qualifizierung zum Datenschutz

Empfehlungen

Anregungen für organisatorische Lösungen:

- Dienstanweisung mit genau beschriebenen Zuständigkeiten und Aufgaben
- Dezentralisierung des Datenschutzes
- Datenschutz als Führungsaufgabe und -qualifikation
- Aufnahme von Datenschutzaufgaben in die Stellenbeschreibungen
- Einbeziehung des Datenschutzes in die Qualitätssicherung; Einsetzung eines Datenschutz-Qualitätszirkels
- Datenschutz als Bestandteil des betrieblichen Weiterbildungsprogramms etablieren
- Ahndung von Verstößen mit Qualifikationsmaßnahmen
- Erstellen eines Datenschutzhandbuchs (Intranet)