nrw.uniTS trifft Datenschutz im Krankenhaus
27. März 2014,
Dr. Bernd Schütze

Zusammenarbeit in der Patientenversorgung – Herausforderung für den Datenschutz?

Zu meiner Person

- Ausbildung
  - Studium Informatik
    (FH-Dortmund)
  - Studium Humanmedizin
    (Uni Düsseldorf / Uni Witten/Herdecke)
  - Studium Jura
    (Fern-Uni Hagen)
  - Zusatzausbildung Datenschutzbeauftragter
    (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - Zusatzausbildung Datenschutz-Auditor
    (TüV Süd)
  - Zusatzausbildung Medizin-Produkte-Integrator
    (VDE Prüf- und Zertifizierungsinstitut)

- Berufserfahrung
  - > 10 Jahre klinische Erfahrung
  - > 20 Jahre IT im Krankenhäusern
  - > 20 Jahre Datenschutz im Gesundheitswesen
- Mitarbeit in Verbänden
  - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
  - Berufsverband Medizinischer Informatiker e.V. (BVMI)
  - Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
  - Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
  - Gesellschaft für Informatik (GI)
  - HL7 Deutschland e.V.
  - Fachverband Biomedizinische Technik e.V. (fbmt)

Datenschutz ?

rson

ung

sern

etrie

S)

chutz und

GDD)

ormatik (GI)

d e.V.

d Biomedizinische Technik

mt)

Cool !!

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Datenschutz: Warum eigentlich?

Der Anfang: Arzt + Patient

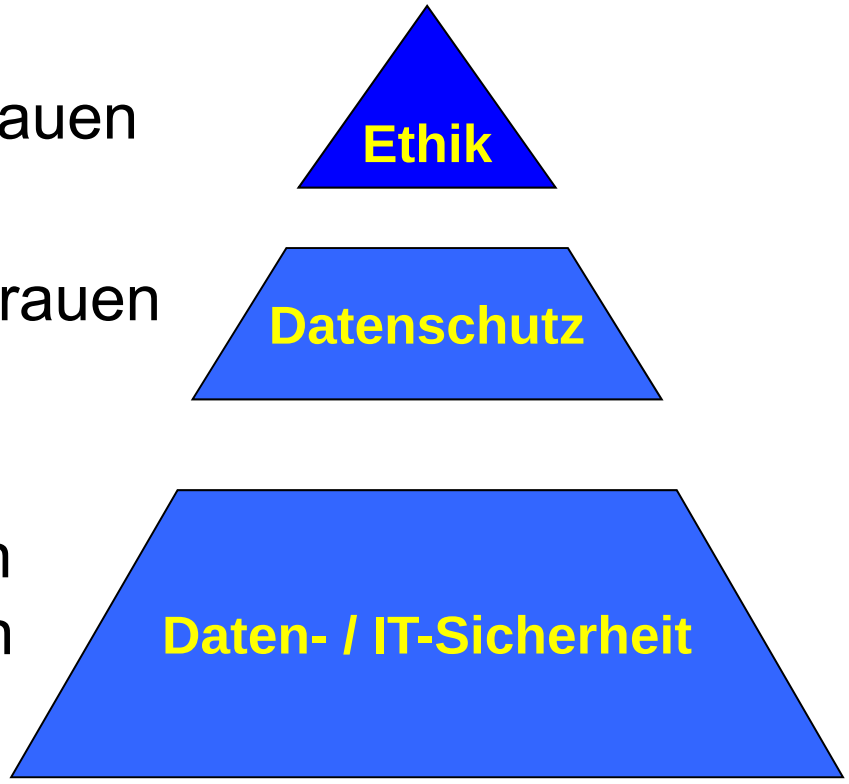
→ Vertrauen

Sie blieben nicht allein:

→ Misstrauen

+ Krankenkasse
+ Verwaltung
+ Vernetzung
+ Fremde

Misstrauen bekämpfen



Grundlage des Datenschutzes

Artikel 1 Grundgesetz

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2 Grundgesetz

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Grundlage des Datenschutzes

Andere Artikel des Grundgesetzes sind nachrangig.

D.h. beispielsweise

Art. 5 Meinungsfreiheit, Freiheit Lehre und Forschung

Art. 10 Briefgeheimnis

sind bzgl. Art. 1 und Art. 2 GG nachrangig.

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

„Volkszählungsurteil“ des BVerfG. von 1983

„Recht auf informationelle Selbstbestimmung“

(BVerfGE 65, 1 – Volkszählung, http://www.servat.unibe.ch/dfr/bv065001.html)

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst.
   Das Grundrecht gewährleistet insoweit die **Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen**.

2. Einschränkungen dieses Rechts auf **"informationelle Selbstbestimmung"** sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Also: Was ist Datenschutz?

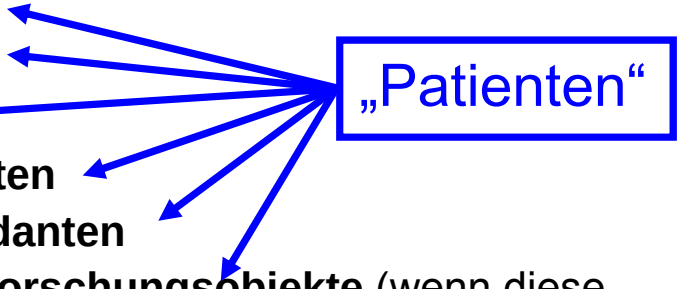
1. Datenschutz ≠ Schutz der Daten

2. Datenschutz = Schutz der Freiheit einer Person, selbst zu entscheiden, was mit ihren/seinen Daten geschieht

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

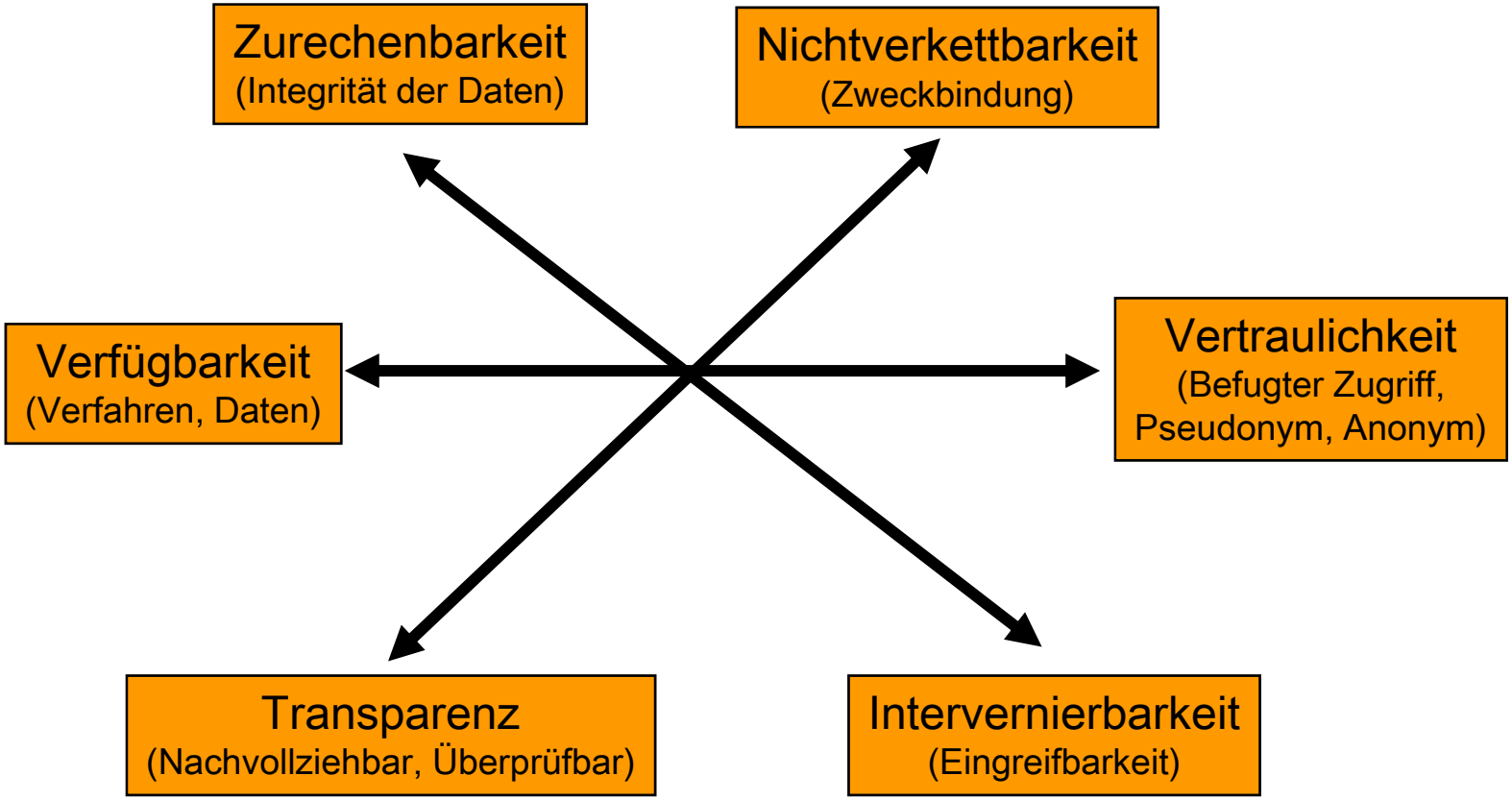
Datenschutz = Personenschutz

- Die Person soll selbst entscheiden, was mit ihren Daten geschieht
- Datenschutz ist überall dort vorhanden, wo eine ***asymmetrische Machtbeziehung*** zwischen Personen und Organisationen existiert:
  - Öffentliche Verwaltung und **Bürger**
  - Private Unternehmen und **Kunden**
  - Arbeitgeber und **Arbeitnehmer**
  - Praxen, Krankenhäuser und **Patienten**
  - Institute, Gemeinschaften und **Mandanten**
  - Wissenschaftsorganisationen und **Forschungsobjekte** (wenn diese Menschen darstellen)
  - Verein und Mitglieder
  - Schule und Schüler
  - …



- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Ziele des Datenschutzes – Antagonisten zueinander?



- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Rechtliche Grundlagen

Bundesrecht
- Bundesdatenschutzgesetz (BDSG)
- Bürgerliches Gesetzbuch (BGB)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Signaturgesetz (SigG)
- Verordnung zur elektronischen Signatur (SigV)
- Mediendienstestaatsvertrag (MDStV)
- …

Landesrecht (z.B. NRW)
- Archivgesetz (ArchivG)
- Gesetz über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz (AG G 10 NW)
- Berufsordnung der Ärztekammer Westfalen-Lippe
- Berufsordnung für die nordrheinischen Ärztinnen und Ärzte
- Berufsordnung für Apothekerinnen und Apotheker der Apothekerkammer Nordrhein
- Berufsordnung für Apothekerinnen und Apotheker derApothekerkammer Westfalen-Lippe
- Datenschutzgesetz (DSG NRW)
- Gesetz über den öffentlichen Gesundheitsdienst (ÖGDG)
- Gesetz über den Feuerschutz und die Hilfeleistung
- Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)
- Gesetz über Tageseinrichtungen für Kinder (GTK)
- Gesundheitsdatenschutzgesetz (GDSG NW)
- Gutachterausschussverordnung (GAVO NRW)
- Heilberufsgesetz (HeilBerG)
- Hochschulgesetz (HG)
- Krankenhausgesetz (KHG NRW)
- Meldedatenübermittlungsverordnung (MeldDÜV NRW)
- Meldegesetz (MG NRW)
- Sicherheitsüberprüfungsgesetz (SÜG NRW)
- Verordnung zur Durchführung des Meldegesetzes (DVO MG NRW)
- …

EU
- Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Richtlinie 2002/22/EG Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie)
- Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)
- Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten
- Richtlinie 2009/136/EG („Cookie“-Richtlinie)
- …

Kirchenrecht
- Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD)
- Verordnung über die in das Gemeindeverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen
- Verordnung über den automatisierten zwischenkirchlichen Datenaustausch
- Verordnung mit Gesetzeskraft zur Einführung des Datenschutzes in der Vereinigten Evangelisch-Lutherischen Kirche Deutschlands
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Anordnung über das kirchliche Meldewesen (KMAO) für Bistum …
- Anordnung über den kirchlichen Datenschutz (KDO) für Bistum …
- Durchführungsverordnung zur KDO (KDO-DVO)
- …

Medizinisches Umfeld
- Musterberufsordnung für deutsche Ärztinnen und Ärzte (MBO)
  - §9 Abs. 1 Schweigepflicht des Arztes
- Strafprozessordnung (StPO)
  - §53 Ab2. 1 Zeugnisverweigerungsrecht
  - §97 Abs.1 Beschlagnahmeverbot
  - §103 Abs.1 eingeschränktes Durchsuchungsrecht für Ärztpraxen
- Strafgesetzbuches (StGB)
  - §203 Abs.1 4.2.1.2.c Ärztliche Schweigepflicht
- Zivilprozessordnung (ZPO)
  - § 383 Zeugnisverweigerung aus persönlichen Gründen
- Sozialgesetzbuch V (SGB V)
  - § 73 Kassenärztliche Vereinigung
  - § 140a Integrierte Versorgung
- …

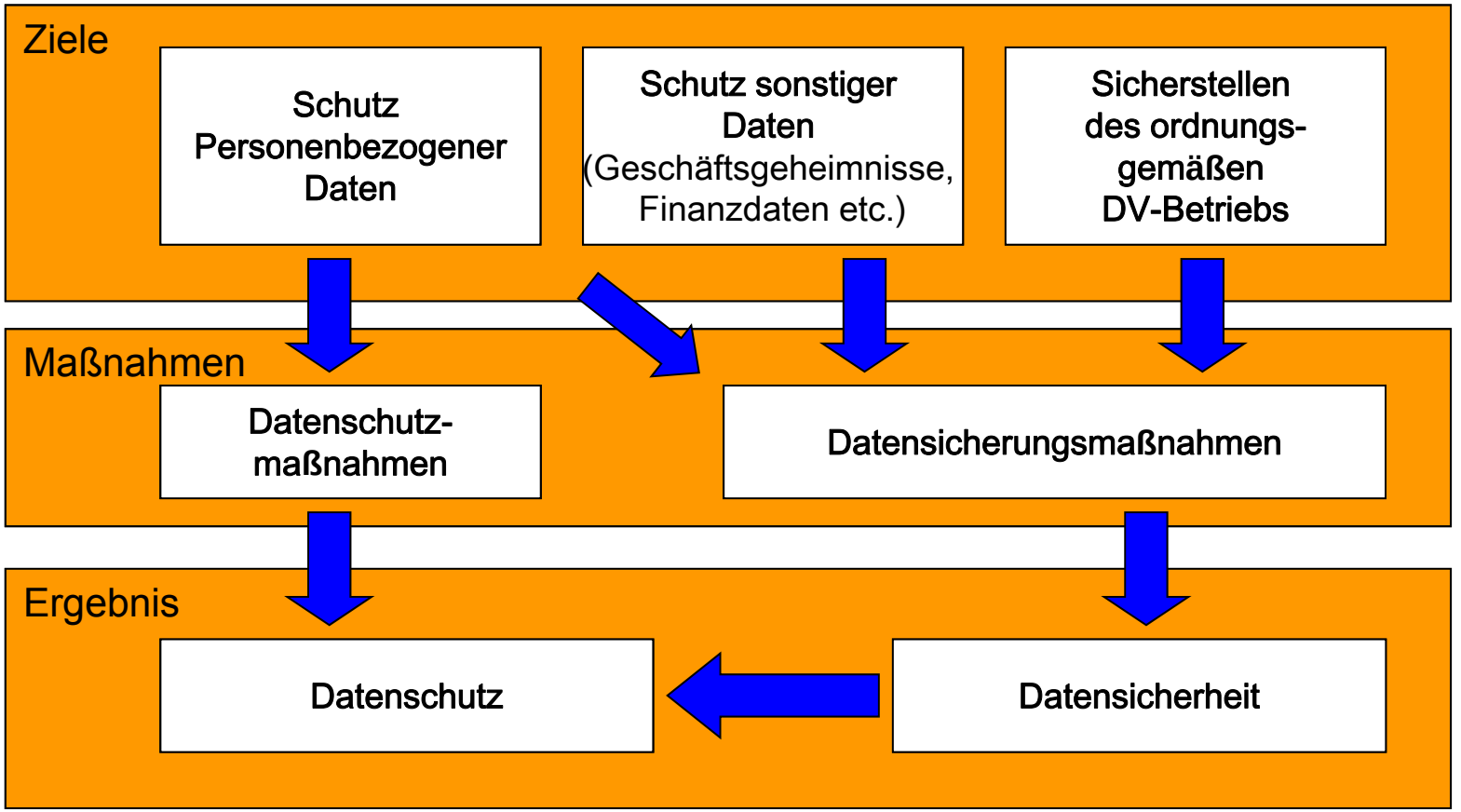
Datenschutz vs. Datensicherheit

- Datensicherheit: Die Person ist der Angreifer!
  - ➔ Die Person muss nachweisen, dass sie kein Angreifer ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss.
- Datenschutz: Die Organisation ist der Angreifer!
  - ➔ Die Organisation muss (jederzeit) prüffähig nachweisen (können), dass sie kein Angreifer ist, sich an die Regeln hält und bei all dem ihre Verfahren und Prozesse beherrscht.

- Dennoch gilt:
  Datenschutz kommt ohne Datensicherheit nicht aus !

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Datenschutz vs. Datensicherheit



- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Die Welt der Normen

Datenschutz

- ISO/TS 25237: Pseudonymisierung
- DIN EN 15713: Sichere Vernichtung von vertraulichen Unterlagen
- DIN EN ISO 27789: Audit-Trails für elektronische Gesundheitsakten
- ISO/TS 22600: Privilegienmanagement und Zugriffssteuerung
- ISO/IEC 15816: Sicherheitsobjekte für Zugriffskontrolle
- ISO/DIS 22857: Leitlinien für den Datenschutz zur Ermöglichung grenzüberschreitender Kommunikation von persönlichen Gesundheitsinformationen
- …

IT-Sicherheit

- ISO/TS 25238: Klassifikation der Sicherheitsrisiken von Software aus dem Bereich Gesundheitswesen
- DIN ISO/IEC 27000: Informationssicherheits-Managementsysteme - Überblick und Terminologie
- DIN ISO/IEC 27001: Informationssicherheits-Managementsysteme - Anforderungen
- DIN ISO/IEC 27002: Leitfaden für das Informationssicherheits-Management
- DIN EN ISO 27799: Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002
- DIN EN 80001: Anwendung des Risikomanagements für IT-Netzwerke mit Medizinprodukten
- …

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

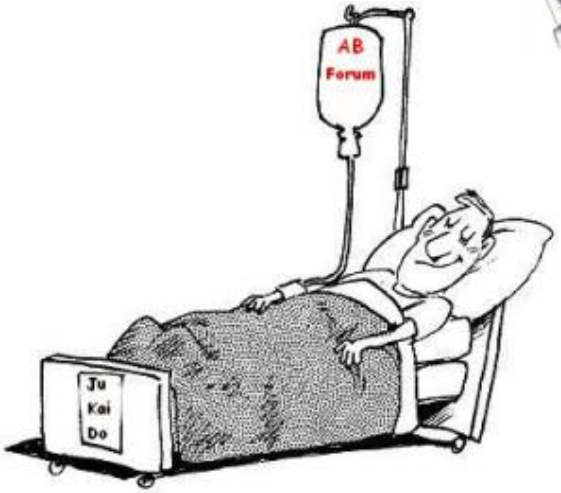
Datenschutz trifft Krankenhaus

Gespräche auf der Arbeit

Unterlagen aus dem Papierkorb
(Z.B. Bewerbung, Arztbrief, …)

Unterlagen auf dem Schreibtisch
(Z.B. Arztbrief, Personalplanung, …)

Angaben zum Patienten
(Z.B. Name, Erkrankung, …)



Angaben zum Personal
(Z.B. Name, Stellung, …)

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Datenschutz trifft Krankenhaus

Externe Dienstleister:
Schreibbüro, Scandienstleistung, Archiv,…

Medizingeräte:
EKG, MRT, CT, BGA, Sono, RR,…

Informationssysteme:
KIS, PACS, RIS, LIS, OIS, …

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Arbeit im Krankenhaus: 1994 und 2014

Z.B.: Abrechnung

Leistungserfassung nach der Patientenversorgung

Leistungserfassung während der Patientenversorgung

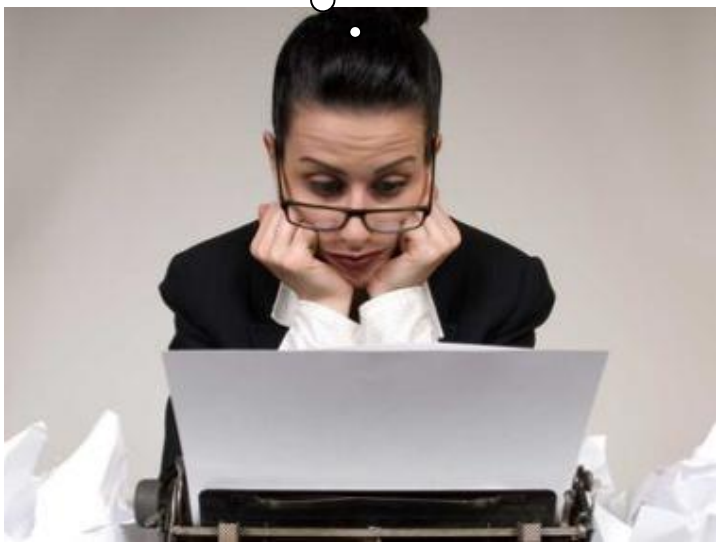
- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Arbeit im Krankenhaus: 1994 und 2014

Z.B.: Arztbriefschreibung

Diktat, Korrekturlesen, erneutes Schreiben, ...

...Anastomose zwischen IMA und RIVA?



- Textbausteine
- Pschyrembel mit Rechtschreibkorrektur
- Automat. Einbindung von Laborwerten, rad. Bilddaten, ...
- Spracherkennung

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Arbeit im Krankenhaus: 1994 und 2014

Z.B.: Archivierung

Riesige Archive mit

- Verlustraten von > 60%
- Anforderungsdauer: z.T. > 2 Tage

Elektronische Archive mit

- Verlustraten < 5%
- Anforderungsdauer: i. d. R. < 1 h

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Arbeit im Krankenhaus: 1994 und 2014

Z.B.: Kommunikation mit Partnern

Datentransfer per Taxi oder Patiententransfer per Krankenwagen

Elektronischer Bild- / Labor- / datenübertragung via Internet

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Arbeit im Krankenhaus: 1994 und 2014

Z.B.: Gesetze

uuups: - da gibt es ja kaum Unterschiede

- Gesundheitsdatenschutzgesetz NRW
- Im Prinzip seit 1994 unverändert
- Wie soll ein 20 Jahre altes Gesetz auf die heutige Arbeitsweise passen?

Aber geändert hat sich im Bereich der Gesetzestexte natürlich schon etwas…

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Das könnte die Politik auch ‘mal modernisieren. Wer ist dafür eigentlich verantwortlich…?

Heutige Herausforderungen

- Arztgeheimnis (§203 StGB) vs. Outsourcing
  - Fernwartung von Medizintechnikgeräten und Informationssystemen
  - Digitalisierung von Patientenakten – externe Scandienstleister erlaubt?
  - …
- Moderne Technik
  - Mobile Geräte (z.B. BYOD u.ä. Fragen)
  - Apps
  - Internet-/Mail-Nutzung
- Vernetzte Gesundheitsversorgung
  - Cloud-Nutzung
  - Einrichtung von Schwerpunktkrankenhäusern = Verstärkte Zusammenarbeit von Krankenhäusern
  - Sektorenübergreifende Versorgung
  - …
- Aktenbasierte einrichtungsübergreifende Bild- und Befund-Kommunikation
  - Elektronische Patientenakten (EPA)
  - Persönliche einrichtungsübergreifende elektronische Patientenakte (PEPA)
  - Fallbezogene einrichtungsübergreifende elektronische Patientenakte (eFA)
  - …
- …

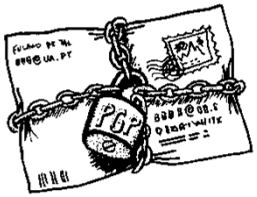
- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion

Meine These

1. Ich bin überzeugt, dass Versorger und Hersteller die Herausforderungen einer modernen Gesundheitsversorgung angehen und meistern (, wenn die Politik sie lässt).
2. Jeder Patient möchte, dass seine Gesundheitsdaten bestmöglich geschützt sind, aber bei Bedarf sollen alle benötigten Daten zur Verfügung stehen.
3. Datenschutz ist daher ein Innovationsmotor, welcher deutschen Lösungen international zum Durchbruch verhelfen kann.

Die folgenden Vorträge liefern Antworten auf einige Fragen…

- Was ist Datenschutz
- Rechtliche Grundlagen
- Datenschutz / Datensicherheit
- Datenschutz im Krankenhaus
- These
- Diskussion



schuetze@medizin-informatik.org
(GPG-Schlüssel auf dem Server abrufbar)