Einführung in Datenschutz und Arztgeheimnis

U. Altmann

Institut für Medizinische Informatik
Justus-Liebig-Universität Gießen

Rudolf-Buchheim-Straße 6, 35392 Gießen
e-Mail: Udo.Altmann@informatik.med.uni-giessen.de
WWW: http://www.akkk.de, http://www.gtds.de

JUSTUS-LIEBIG-
UNIVERSITÄT
GIESSEN

Gliederung

- Grundgedanken (Prinzipien und Grenzen) von
  - Datenschutz
  - Arztgeheimnis
- Gesetze
  - Quiz
- Datenschutzgesetzgebung
  - praktisches Beispiel: Krebsregister
- Datenschutz im Krankenhaus
  - Technische Maßnahmen
  - Grundbegriffe der Kryptografie

Grundgedanken des Datenschutzes

- Grundgesetz Art. 2 Abs. 1:
  - Freie Entfaltung der Persönlichkeit
    => Schutz der Privatsphäre
    => Recht auf „informationelle Selbstbestimmung“
    (Volkszählungsurteil 1983)
- Recht nicht schrankenlos
  - Allgemeininteresse
  - Öffentliche Aufgaben erfordern persönliche Daten
- Güterabwägung / Verhältnismäßigkeit

Zweck von Gesetzen und Schutzvorschriften

- bestimmen Voraussetzungen für Datenverarbeitung
- Grundsatz: erlaubt ist nur
  - was ausdrücklich (durch Vorschrift) gestattet
  - oder (!) wozu der Betroffene schriftlich seine Einwilligung erklärt hat
    => z.B. Datenschutzerklärung in klinischen Studien
- Umfasst auch alle Arten von Akten einschließlich multimediale Inhalte
- Grundsatz: Erhebung
  - nur erforderlicher Umfang
  - Mitteilungspflicht
  - aber: Ausnahmeregelungen
- Grundsatz: Zweckbindung
  - Daten nur für den Zweck verwenden, für die sie erhoben worden sind
  - aber: Ausnahmeregelungen
- Grundsatz: Bürger (Patient) hat (i.d.R. kostenloses) Auskunftsrecht

Arztgeheimnis

- (Muster-)Berufsordnung
  - Umsetzung in Berufsordnungen der Landesärztekammern
- Grundsätze älter als alle Datenschutzgesetze
- gilt ergänzend zum Datenschutz

(Muster-)Berufsordnung §9 Schweigepflicht

(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist - auch über den Tod des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(2) Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht des Arztes einschränken, soll der Arzt den Patienten darüber unterrichten.

Bruch der Schweigepflicht

- Offenbarungs**recht**
  - ausdrückliche Entbindung / stillschweigende oder mutmaßliche Einwilligung
  - Gefahrenabwehr (Straßenverkehr, HIV-Infektion, Kindesmißhandlung, Eigen-/Fremdgefährdung)
    => Ultima ratio / erfordert ausführliches Gespräch
- Offenbarungs**pflicht**
  - Im allgemeinen durch spezielle Gesetze (STGB, StVollzG, StPO, SGB, …) geregelt
  - Z.B. Meldepflichten bei Infektionserkrankungen, im Rahmen von Leichenschau …

Wichtige Offenbarungsrechte des Arztes I

Quelle: Deutsches Ärzteblatt, Jg. 102, Heft 5
4. Februar 2005

- Rechtfertigungsgründe aus der Sphäre des Patienten
  - Entbindung von der Schweigepflicht (Einverständnis bzw. Einwilligung)
  - Stillschweigende Einwilligung im Rahmen der Sozialadäquanz
    - Information des weiter- beziehungsweise nachbehandelnden Arztes
    - Information des Konsiliarius
  - Mutmaßliche Einwilligung
    - Bewusstloser Patient gegenüber Angehörigen, wenn kein gegenteiliger Wille bekannt ist.
    - Verstorbener Patient gegenüber Angehörigen, zum Beispiel zur Geltendmachung von Unterhaltsansprüchen, wenn kein gegenteiliger Wille bekannt ist.
- Nicht (beispielsweise)
    - Befreundete Ärzte, Praxisübernahme, Kantine, …

Wichtige Offenbarungsrechte des Arztes II

Quelle: Deutsches Ärzteblatt, Jg. 102, Heft 5
4. Februar 2005

- Rechtfertigungsgrund des rechtfertigenden Notstands nach § 34 StGB zum Schutz höherrangiger Rechtsgüter
  - Kindesmisshandlung und Kindesmissbrauch
  - Fremdgefährdung im Straßenverkehr
  - Offenbarung psychischer Erkrankungen zum Zwecke der Unterbringung bei Eigen- und Fremdgefährdung (siehe auch spezialgesetzliche Regelungen)
  - Unterrichtung des Partners über die Erkrankung des Lebensgefährten an HIV (strittig) siehe Offenbarungspflichten

(Muster-)Berufsordnung §9 Schweigepflicht

(3) Der Arzt hat seine Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

(4) Wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist.

(Muster-)Berufsordnung §10 Dokumentationspflicht

…

(5) Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Der Arzt hat hierbei die Empfehlungen der Ärztekammer zu beachten.

(Muster-)Berufsordnung §15 Forschung

…

(2) Zum Zwecke der wissenschaftlichen Forschung und Lehre dürfen der Schweigepflicht unterliegende Tatsachen und Befunde grundsätzlich nur soweit offenbart werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt.

Gesetze

- Strafgesetzbuch
  - Verletzung (§203) und Verwertung (§204) von Geheimnissen
- Bundesdatenschutzgesetz
- Landesdatenschutzgesetze
- EU-Datenschutzgrundverordnung (EU-DSGVO)
  - gilt als Grundlage für EU-Länder(anzuwenden ab 25. Mai 2018)
  - zahlreiche Gesetze und Verordnungen müssen angepasst werden
  - in Folge auch Verträge und Datenschutzhinweise
- sowie zahlreiche Gesetze und Verordnungen, die für bestimmte Anwendungsbereiche
  - Datenerhebungen erlauben
  - Umgang mit Daten regeln
  - siehe http://www.datenschutz.de

Strafgesetzbuch
§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

…

anvertraut worden oder sonst bekanntgeworden ist, wird mit **Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe** bestraft.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis **nach dem Tod** des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe **Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe**.

Strafgesetzbuch
§ 204 Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit **Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe** bestraft.

(2) § 203 Abs. 4 gilt entsprechend.

10 Quizfragen

Quelle: Deutsches Ärzteblatt, Jg. 102, Heft 5
4. Februar 2005

3 Punkte cme

Dieser Beitrag wurde von der Nordrheinischen Akademie für ärztliche Fort- und Weiterbildung zertifiziert.

Eine Teilnahme an der zertifizierten medizinischen Fortbildung im Deutschen Ärzteblatt ist nur im Internet möglich, unter der Adresse:

www.aerzteblatt.de/cme

Zertifizierte Medizinische Fortbildung

Die ärztliche Schweigepflicht

Markus Parzeller[1, 2], Maren Wenk[1], Markus A. Rothschild[3]

Zusammenfassung

Welche Aussage(n) zur Geschichte der ärztlichen Schweigepflicht trifft/treffen zu?

1) Der Eid des Hippokrates regelt für jeden Arzt rechtsverbindlich die ärztliche Schweigepflicht.
2) Die Ausführung des Eides des Hippokrates zur ärztlichen Schweigepflicht entfaltet keine rechtsverbindlichen Auswirkungen für den Arzt.
3) In der Antike wurde die ärztliche Schweigepflicht als „Heilige Pflicht“ beschrieben.
4) Die Regelung der ärztlichen Schweigepflicht im Eid des Hippokrates lässt sich als Vorläufer heutiger moderner Gesetze werten.

a) Nur 1 trifft zu
b) Nur 1 und 3 treffen zu
c) Nur 2, 3 und 4 treffen zu
d) Nur 4 trifft zu
e) Nur 2 trifft zu

Verfassungsrechtlich und einfach gesetzlich hat die ärztliche Schweigepflicht folgende Grundlagen:

1) Recht auf informationelle Selbstbestimmung (Art. 1 I i.V. m. Art. 2 I GG)
2) Schutz von Privatgeheimnissen gemäß §§ 203 ff. StGB
3) Zivilrechtliche Nebenpflicht des Arzt-Patienten-Vertrages
4) Berufs- und standesrechtliche Regelung
5) Nebenpflicht zur Verschwiegenheit im Arbeitsverhältnis

a) Alle treffen zu
b) Nur 1, 2 und 4 treffen zu
c) Nur 2 und 5 treffen zu
d) Nur 3 und 4 treffen zu
e) Nur 1, 3 und 5 treffen zu

Zum schweigepflichtigen Personenkreis des § 203 StGB gehört nicht:

a) Zahnarzt

b) Apotheker

c) Heilpraktiker

d) Arzt

e) Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert

Eine Befugnis zur Offenbarung von Patientendaten ohne Entbindung ist vor folgenden Berufsgruppen jederzeit zulässig:

a) Staatsanwälten

b) Richtern

c) Polizeibehörden

d) Ärzten

e) Keine Angabe ist richtig

Eine Befugnis zur Offenbarung von Patientendaten ist aus der Sphäre des Patienten zulässig bei:

1) ausdrücklicher Entbindung durch den Patienten
2) mutmaßlicher Einwilligung des bewusstlosen Patienten
3) mutmaßlicher Einwilligung des verstorbenen Patienten
4) stillschweigender Einwilligung im Rahmen der Sozialadäquanz

a) Nur 1 und 3 treffen zu
b) Nur 1 und 2 treffen zu
c) Nur 3 und 4 treffen zu
d) Nur 2 und 4 treffen zu
e) Alle treffen zu

Gegen den erklärten oder mutmaßlichen Willen des Patienten darf die ärztliche Schweigepflicht

1) als eine der höchsten Berufspflichten nie gebrochen werden.
2) bei Gefährdungen des Straßenverkehrs durch den uneinsichtigen Patienten immer gebrochen werden (Schutz der Allgemeinheit).
3) bei Vergewaltigungsdelikten immer gebrochen werden.
4) bei Gefahren für ein anderes Rechtsgut von hohem Rang gegebenenfalls nach einer warnenden Stufenabfolge gebrochen werden.

a) Nur 1 und 3 treffen zu
b) Nur 2 und 4 treffen zu
c) Nur 1, 2 und 3 treffen zu
d) Nur 4 trifft zu
e) Alle treffen zu

Bei Ihnen wird ein Patient mit einer frischen Schussverletzung eingeliefert.
Was gilt bezüglich Ihrer Schweigepflicht beziehungsweise Offenbarungsbefugnis?

1) Schussverletzungen müssen der Polizeibehörde gemeldet werden, wenn es sich bei dem Patienten um einen angeschossenen Straftäter handelt.
2) Schussverletzungen müssen der Polizeibehörde gemeldet werden, wenn es sich bei dem Patienten um das Opfer einer Straftat handelt.
3) Schussverletzungen müssen der Polizeibehörde gemeldet werden, wenn es sich um einen bewusstlosen Patienten handelt.
4) Schussverletzungen dürfen der Polizeibehörde gemeldet werden, wenn es sich um einen bewusstlosen Patienten (mutmaßliche Einwilligung) handelt.

a) Nur 1, 2 und 3 treffen zu
b) Nur 1, 2 und 4 treffen zu
c) Nur 2, 3 und 4 treffen zu
d) Nur 2 und 3 treffen zu
e) Nur 4 trifft zu

Zur Rechtfertigung einer Offenbarung des Arztgeheimnisses gegen den Willen des Patienten müssen im Anwendungsbereich des § 34 StGB (rechtfertigender Notstand) folgende Voraussetzungen vorliegen:

1) Die Offenbarung muss das mildeste Mittel darstellen.
2) Es müssen eindringliche Gespräche mit dem Patienten zur Selbstoffenbarung oder Unterlassung gefährlicher Handlungen stattgefunden haben (Ausnahme: unverzügliches Handeln erforderlich).
3) Der Arzt muss eine genaue Kenntnis der rechtfertigenden Umstände haben.
4) Es muss eine gegenwärtige Gefahr für die Rechtsgüter des Arztes oder eines Dritten bestehen.

a) Nur 2, 3 und 4 treffen zu
b) Nur 2 und 3 treffen zu
c) Nur 1 und 4 treffen zu
d) Alle Angaben sind richtig
e) Alle Angaben sind falsch

Im Arbeitsrecht muss der Arzt bezüglich der ärztlichen Schweigepflicht Folgendes beachten:

1) Der Arbeitgeber des Patienten hat einen Anspruch auf Mitteilung der wichtigsten Diagnosen.
2) Der Arbeitgeber des Patienten hat keinen Anspruch auf Mitteilung der wichtigsten Diagnosen.
3) Die Krankenhausverwaltung hat ein generelles Einsichtsrecht in die Patientenunterlagen des Krankenhauses.
4) Die Krankenhausverwaltung hat kein generelles Einsichtsrecht in die Patientenunterlagen des Krankenhauses.

a) Nur 1 und 4 treffen zu
b) Nur 2 und 4 treffen zu
c) Nur 1 und 3 treffen zu
d) Nur 2 und 3 treffen zu
e) Nur 2 trifft zu

Standes- und berufsrechtlich ist für den Arzt Folgendes zur ärztlichen Schweigepflicht zu beachten:

1) Rechtsverbindlich ist für ihn die aktuelle Version der Musterberufsordnung der Bundesärztekammer.
2) Rechtsverbindlich ist für ihn die aktuelle Version der jeweiligen landesspezifischen Berufsordnung (Bundesland der Berufausübung).
3) Ein rechtswidriger Verstoß gegen die Schweigepflicht ist standesrechtlich unbeachtlich.
4) Ein rechtswidriger Verstoß gegen die Schweigepflicht führt zwingend zur Berufsunwürdigkeit.
5) Ein rechtswidriger Verstoß gegen die Schweigepflicht kann standesrechtlich geahndet werden.

a) 1 und 2 treffen zu
b) 2 und 5 treffen zu
c) 3 und 5 treffen zu
d) 1, 3 und 4 treffen zu
e) 1, 2 und 4 treffen zu

Bundesdatenschutzgesetz

- Entspricht ehemals der europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995
  - Jetzt angepasst an die EU-DSGVO
- Geltungsbereich
  - Öffentliche Stellen des Bundes
    - „öffentlich“ umfaßt auch „abhängige“, „beauftragte“ Institutionen
  - Nur eingeschränkt öffentliche Stellen der Länder (Bundesaufgaben) => Landesdatenschutzgesetze
  - Nicht öffentliche Stellen (Ausnahme persönlicher/familiärer Bereich)

Landesdatenschutzgesetz Beispiel Hessen

- Geltungsbereich
  - Öffentliche Stellen der Länder
    (sofern sie nicht Bundesaufgaben wahrnehmen
    => Bundesdatenschutzgesetz)
  - d.h. Krankenhäuser, wenn „öffentlich-rechtlich“
    - sonst Bundesdatenschutzgesetz oder spezielle Normen (kirchliche Datenschutzgesetze)
    - andernorts evtl. in speziellen Gesetzen geregelt
    - Grundsätze aber überall vergleichbar (=> EU-DSGVO)
  - Hessen hat das formell erste Datenschutzgesetz der Welt (1970)

Besonderer Datenschutz

- ...
- §33 (HDSG) Datenverarbeitung für wissenschaftliche Zwecke
  - personenbezogene Daten dürfen verarbeitet werden wenn
  - schutzwürdige Interessen nicht betroffen
  - öffentliches Interesse überwiegt, Ergebnis nicht anders erreichbar (Regelungen!)
  - Zweckbindung, frühest mögliche Abtrennung identifizierender Daten, ggf. Anonymisierung
- ...

Anonymisierung und Pseudonymisierung

- Anonymisierung
  - Person ist nicht oder nur mit unverhältnismäßig hohem Aufwand wieder identifizierbar
    - z.B. Zusatzwissen, was normalerweise nicht vorliegt
- Pseudonymisierung
  - Identifizierende Daten nur mit Kenntnis einer „Umkehrfunktion“ wieder herstellbar
    - kann notwendig sein für Zusatzinformationen, die sich im Laufe eines Projekts als erforderlich erweisen
- Problematik Zeitverlauf
  - zu unterschiedlichen Zeitpunkten erhobene Daten müssen einem Fall zugeordnet werden
  - teilweise komplexe technische Lösungen

Anonymisierung und Pseudonymisierung - Beispiel

Rohdaten

ID	Name	Vorname	Geburtsdatum	Krebs	Alkoholiker	HIV-Infiziert	Schizophrenie	Groesse
1	Meier	Anton	01.01.1978	Nein	Ja	Nein	Ja	178
2	Müller	Bert	03.03.1979	Ja	Nein	Nein	Nein	179
3	Schulze	Claus	05.05.1960	Ja	Nein	Nein	Ja	165
4	Muster	Dieter	07.07.1968	Nein	Ja	Ja	Nein	195

Zusammenführen von Daten und Nacherhebung

Auswerten

Ident-Daten

ID	Name	Vorname	Geburtsdatum
1	Meier	Anton	01.01.1978
2	Müller	Bert	03.03.1979
3	Schulze	Claus	05.05.1960
4	Muster	Dieter	07.07.1968

Medizinische Daten

ID	Krebs	Alkoholiker	HIV-Infiziert	Schizophren	Groesse
1	Nein	Ja	Nein	Ja	178
2	Ja	Nein	Nein	Nein	179
3	Ja	Nein	Nein	Ja	165
4	Nein	Ja	Ja	Nein	195

Sind diese Daten anonym?

Medizinische Daten

ID	Krebs	Alkoholiker	HIV-Infiziert	Schizophren	Groesse
1	Nein	Ja	Nein	Ja	178
2	Ja	Nein	Nein	Nein	179
3	Ja	Nein	Nein	Ja	165
4	Nein	Ja	Ja	Nein	195

- Namen stehen nicht drin, aber mit dem Zusatzwissen
  - Mein Nachbar Anton Meier ist in der Liste.
  - Mein Nachbar ist 178 cm groß.
- weiß ich dass er alkoholkrank ist und an Schizophrenie leidet, wenn mir nur die medizinischen Daten vorliegen

Anwendungsbeispiel Krebsregister

- Grundlagen und Anwendung von Datenschutz in Krebsregistern
  - Berechtigung ein Register aufzubauen
  - Warum gibt es keine Alternative?
  - Werden personenidentifizierende Daten benötigt?
  - Rechtliche Verfahrensbestimmungen

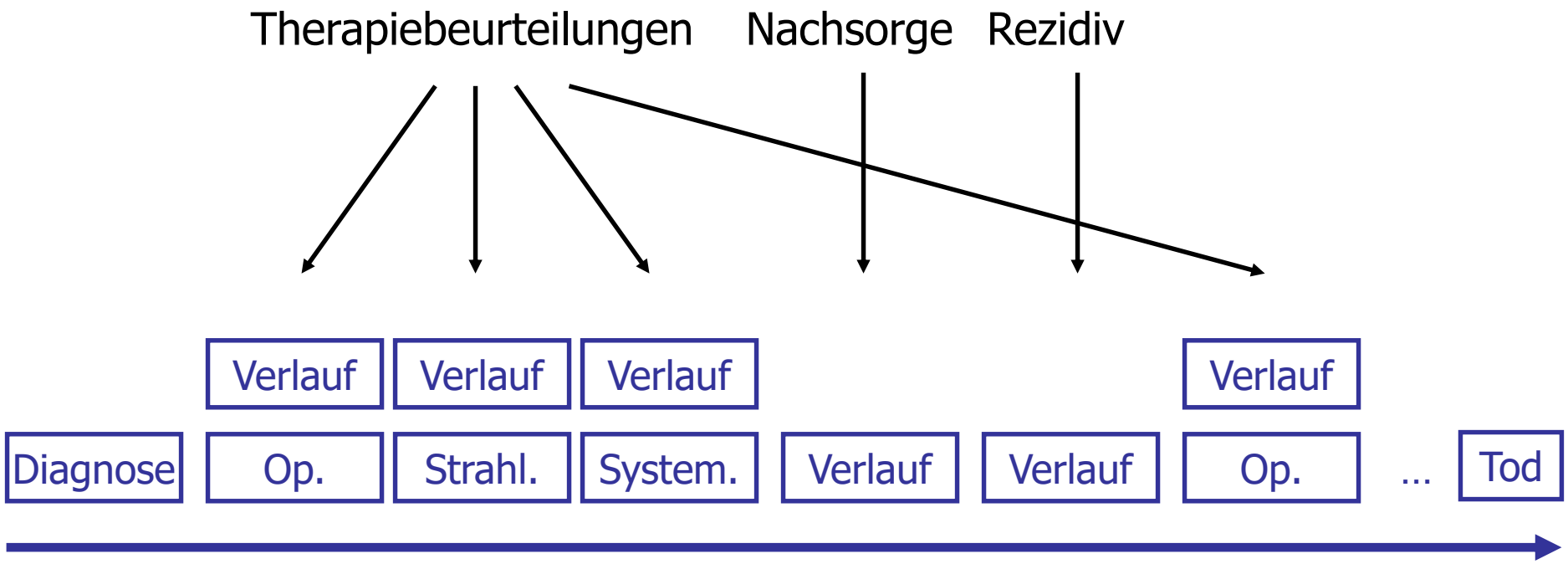
Anwendungsbeispiel: Datenschutz in Krebsregistern (I)

- Was ist die Aufgabe eines Krebsregisters?
  - Epidemiologie
    - Inzidenzbestimmung für Tumorerkrankungen
      - Vergleich im zeitlichen Verlauf und in Bezug auf Regionen
      - => Erkennung von Krebsgefährdungen, Hypothesenbildung
    - Unterstützung epidemiologischer Studien
      - Kohortenabgleich z.B. im Rahmen von Screening
      - detaillierte Risikoanalyse erkrankter vs. nicht Erkrankter (Fall-Kontroll-Studien)
  - Qualitätssicherung
    - Z.B. Einhalten von Leitlinien
  - Unterstützung Versorgung
    - Erinnerungsverfahren
  - Versorgungsforschung
    - Wie wirken Therapien außerhalb von Studienbedingungen

Anwendungsbeispiel: Datenschutz in Krebsregistern (II)

- Mit welcher Begründung wird die Etablierung von Krebsregistern gerechtfertigt?
  - Öffentliches Interesse: Maßnahmen zur Krebsbekämpfung
    - planen, unterstützen, überwachen, evaluieren
- Kann das Ziel auf anderen Wegen erreicht werden?
  - allenfalls punktuell bei besonderen Fragestellungen
  - im Allgemeinen jedoch nicht, da die Daten sonst nirgendwo vorliegen

Krebsregistrierung – Meldeanlässe



Anwendungsbeispiel: Datenschutz in Krebsregistern (III)

- Welches sind die Quellen von Krebsregistern?
  - Meldungen von Pathologen
    - Können prinzipiell kein Einverständnis holen
  - Klinische Meldungen von betreuenden Ärzten/Zahnärzten
  - Leichenschauscheine
    - Aufdeckung zu Lebzeiten nicht gemeldeter Fälle (DCN/DCO)
    - Bestimmung von Mortalitätsraten und Überlebenszeiten
- Was ist problematisch, wenn mehrere Meldungen zu einem Tumor eintreffen?
  - Zusammenführung von Daten
    => Vermeiden von Über-/Unterzählungen
  - Auflösen von Widersprüchen in Daten
  - Personenbezug muß hergestellt werden

Anwendungsbeispiel: Datenschutz in Krebsregistern (IV)

- Zu welcher Datenschutzforderung steht die Notwendigkeit des Personenbezugs im Widerspruch?
  - frühest mögliche Abtrennung identifizierender Daten, ggf. Anonymisierung
- Für welche Aufgabe ist eine Personenidentifikation unerläßlich?
  - Durchführen von Studien, die weitergehende Daten zu Person (z.B. Risikofaktoren) erfordern
  - Unterstützung der Versorgung

Hessisches Krebsregister

- Gesetzlich geregelt
  - Begründung öffentliches Interesse
  - Meldepflicht für Ärzte
    - wichtige Motivationsgrundlage, selbst wenn nicht sanktionsbewehrt
  - Unterrichtung des Patienten (wenn nicht möglich Begründung)
  - Widerspruchsrecht des Patienten
  - Trennung Auswertungsbereich (Registerstelle) von Datenhaltungsbereich (Vertrauensstelle)
    - In Auswertungsbereich ist Personenidentifikation entfernt

Datenschutz ist mehr als Vertraulichkeit

- Aspekt Datensicherheit
  - Richtigkeit / Unverfälschbarkeit
  - Verfügbarkeit
  - Datensicherung
- Aspekt Organisation
  - Räumliche Zugriffsbeschränkungen etc.
  - Hierarchien
- Protokollierung und Kontrolle
  - Was muss/darf protokolliert werden

Datenschutz im Krankenhaus

- Kooperation mehrerer Ärzte, unterschiedlicher Fachabteilungen und Berufsgruppen
  - aus Praktikabilitätsgründen kann nicht von jeder „Geheimnisweitergabe“ eine Erlaubnis eingeholt werden
  - trotzdem gilt „Minimalitätsprinzip“
- Ärztliche Dokumentationspflicht erfordert Datenerhebung und Speicherung/Archivierung über bestimmte Zeiträume
  - => Grundprinzipien für Software

„besondere Kategorien personenbezogener Daten“ nach BDSG §46 (Umsetzung EU-Richtlinie)

- Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten und
- Daten zum Sexualleben oder zur sexuellen Orientierung

Kommt fast alles in der Medizin vor! Hoher Schutzanspruch

Arten von Patientendaten
unterschiedliche „Sensibilität“

- **Identifikationsdaten** (Name, Geburtsdatum, Adresse, evtl. Krankenkassennummer, sowie krankenhausinterne Identifikatoren)
- **administrative Daten („Abrechnung“)**:
  - Versicherungsdaten
  - Bewegungsdaten (Aufnahme, Verlegung, Entlassung)
  - weitere fallbezogene Daten, z. B. Wahlleistungen
- **medizinische Daten („Versorgung“)**:
  - Notfalldaten
  - allgemeine anamnestischen Daten
  - abrechnungsrelevante Diagnosen und Therapien
  - Befunde, Laborwerte und andere diagnostische und therapeutische Daten
  - besonders sensible Daten (z. B. psychiatrische Daten, sexuelle Orientierung, bestimmte Befunde)
  - genetische Daten

Arten von Rechten
(müssen in EDV abbildbar sein)

- Rechte werden erteilt auf Zugehörigkeit zu
  - Fachabteilung
  - Rolle (Arzt, Pflege, …)
  - oder an individuell Einzelpersonen
- Voraussetzung Behandlungszusammenhang
  - Umfasst Aufenthalt + Zeitraum zur Arztbriefschreibung
  - Notfallzugriff mit Protokollierung möglich
  - außerhalb nur Zugriff für (definierte) wissenschaftliche Zwecke / Qualitätssicherung (Minimierung und frühzeitige Pseudonymisierung/Anonymisierung)
- Ausformulierung im einzelnen Krankenhaus bestimmt durch
  - Vereinbarungen des Management, Abstimmung mit Datenschutzbeauftragten des Krankenhauses
  - Besondere Verfahren (z.B. Krebsregister) müssen mit (meist Landes-) Datenschutzbeauftragten abgestimmt werden

Technische Maßnahmen

- Zugang zu System nur mit Authentifizierung
  - Benutzerkennung / Passwort (unsicher)
  - besser: Health Professional Card
    (aber noch nicht flächendeckend eingeführt)
  - (biometrische Systeme? Iriserkennung, Fingerabdruck, …)
- Innerhalb der System möglichst Trennung verschiedener Datenbereiche
  - z.B. personenidentifizierende/medizinische/besonders sensible medizinische Daten
  - Reduzierung der Gefahr unerlaubten Zugriffs von Seiten der EDV-Administration

Ziele der Kryptografie
(nach http://de.wikipedia.org/wiki/Kryptografie)

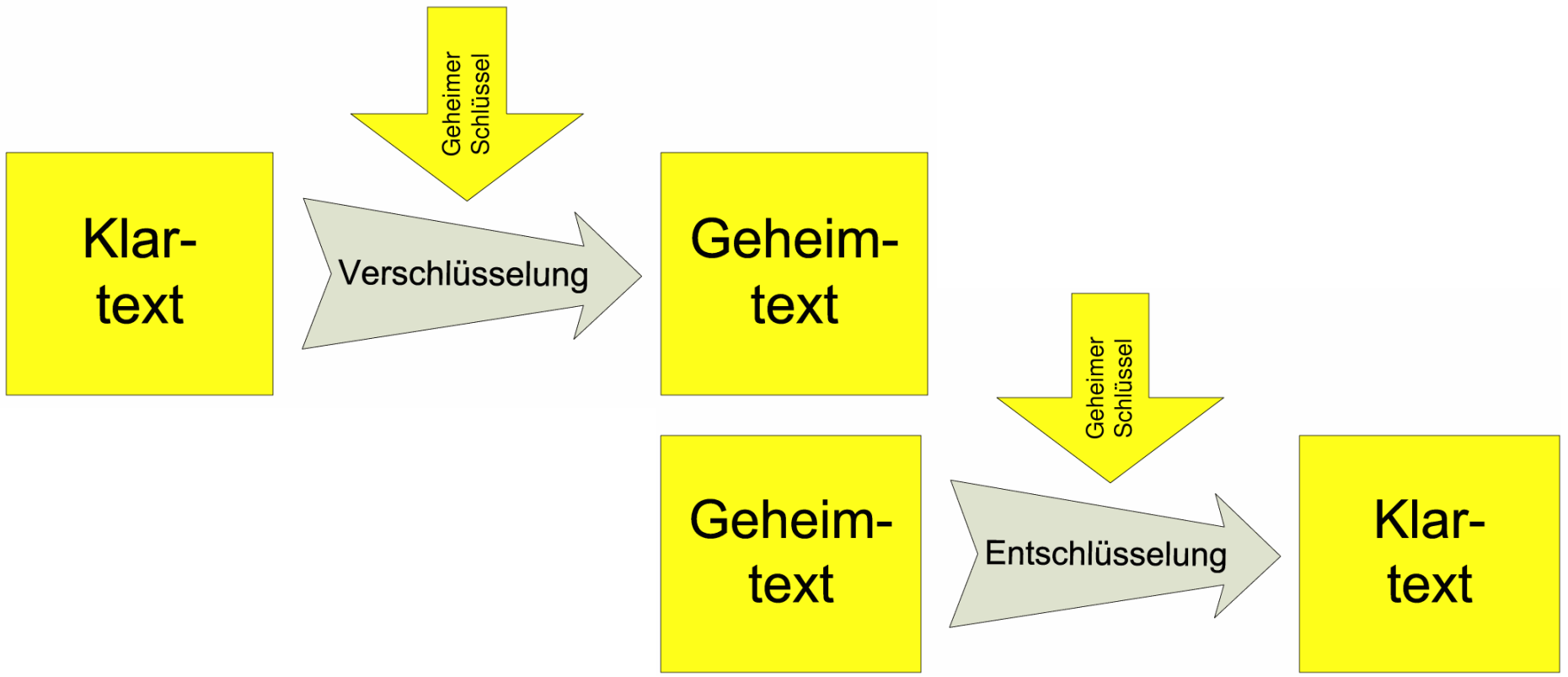
- Vertraulichkeit der Nachricht
  - Schutz vor fremdes Lesen
- Datenintegrität der Nachricht
  - Schutz vor Verfälschung von Inhalten
- Authentifizierung
  - Ist der Absender wirklich der behauptete?
- Verbindlichkeit
  - Absender kann die Nachricht nicht bestreiten

Methoden der Verschlüsselung

- Symmetrische Verfahren
  - **ein** Schlüssel („Geheimnis“) zum Chiffrieren und Dechiffrieren
  - keine Signatur (elektronisches Unterschreiben) möglich
    - Geheimnis mehrerer Personen
    - => keine Authentifizierung und keine Verbindlichkeit
- Asymmetrische Verfahren
  - **zwei** Schlüssel (Schlüsselpaar) **pro Benutzer**
    - **einer** zum Dechiffrieren von Nachrichten an Benutzer bzw. Signieren von Dokumenten des Benutzers (**privat**, geheim)
    - **einer** zum Chiffrieren von Nachrichten an Benutzer bzw. Überprüfen einer Signatur von Dokumenten des Benutzers (**öffentlich**)

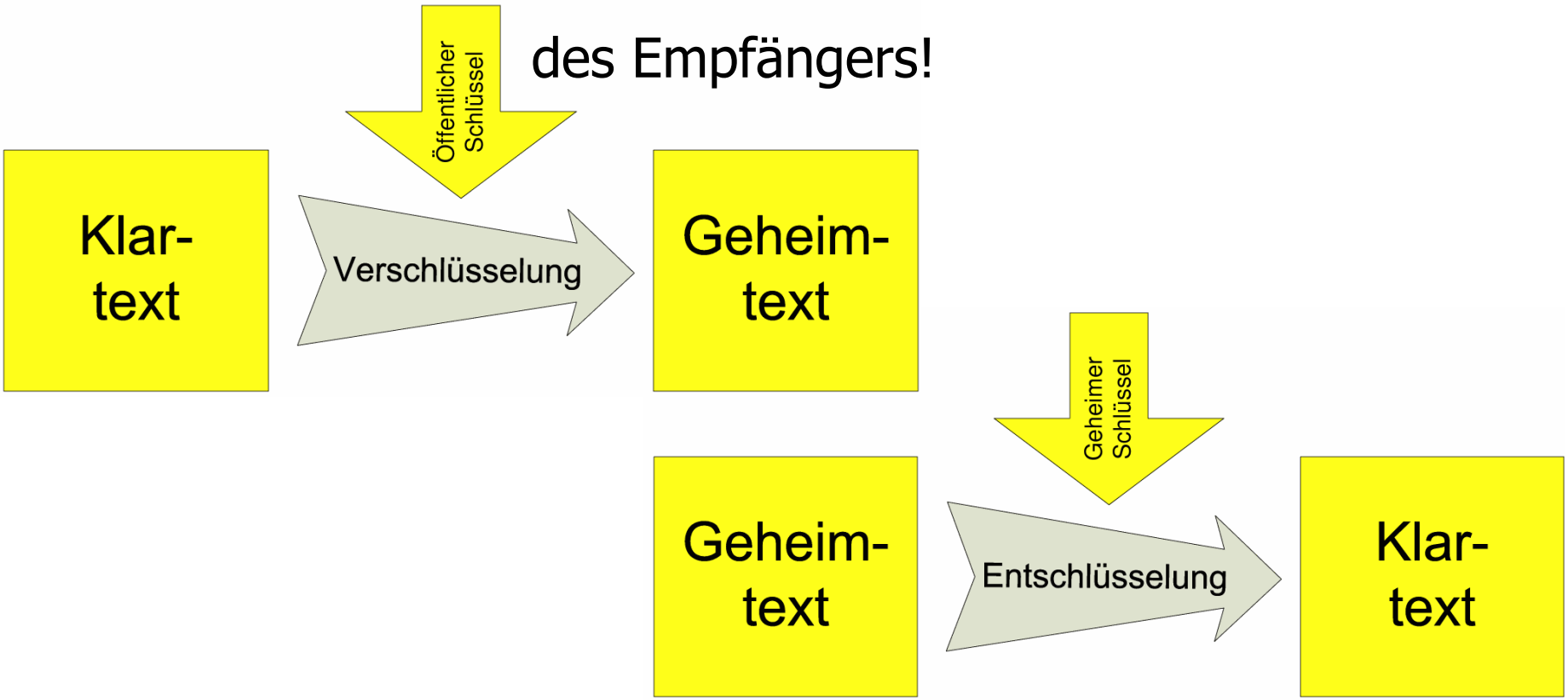
Symmetrische Verfahren

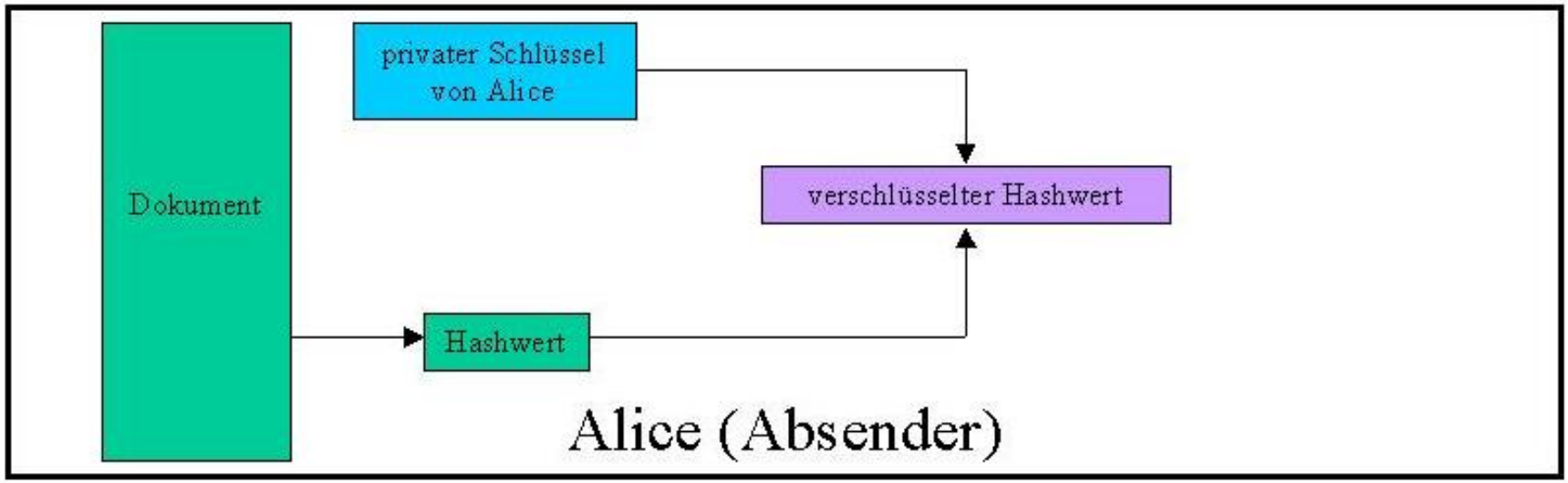
(nach http://de.wikipedia.org/wiki/Symmetrische_Verschl%C3%BCsselung)



Asymmetrische Verfahren

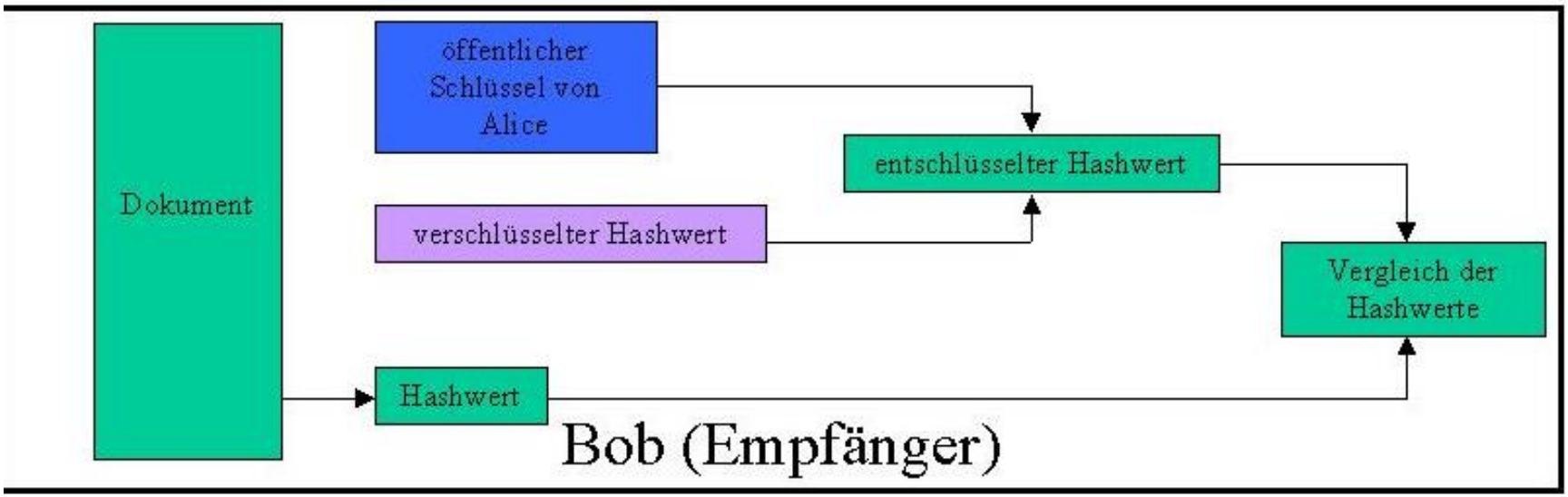
(http://de.wikipedia.org/wiki/Asymmetrische_Verschl%C3%BCsselung)





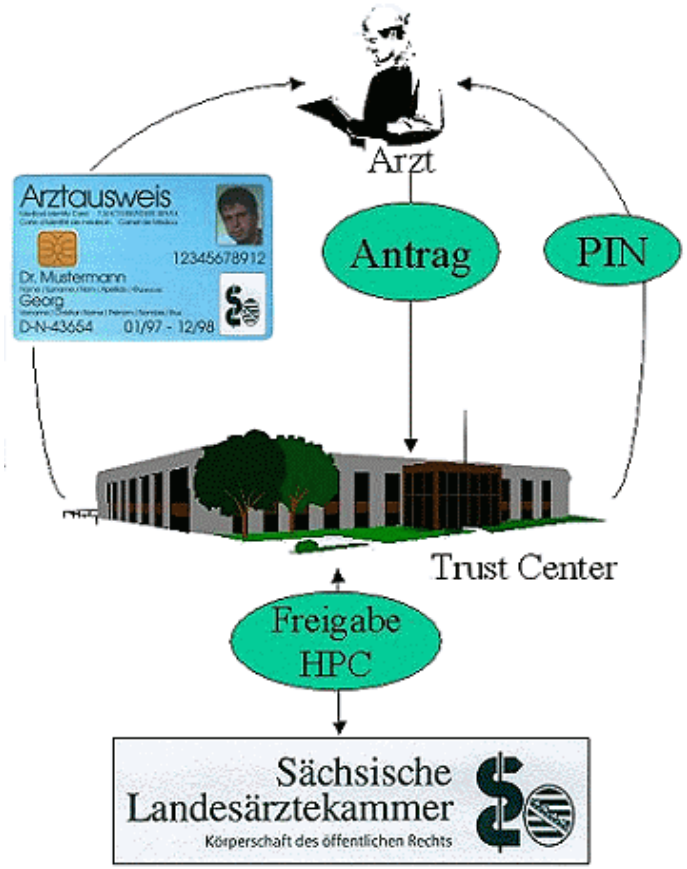
Asymmetrische Verfahren als Signatur

(http://de.wikipedia.org/wiki/Elektronische_Signatur)



Möglichkeiten der Health Professional Card (elektronischer Arztausweis) für Datenschutz

- Authentifizierung
  - Eindeutige Identifikation von Benutzern
- Bereitstellung von Schlüsseln für
  - Kryptographie von Inhalten (bei Speicherung oder während des Transports von Daten über Netzwerke)
  - Signatur (Unterschrift) von Inhalten
- Erfordert (aufwendige) Public Key Infrastruktur (PKI)



Zusammenfassung

- Datenschutz ist ein (gesetzlich geregeltes und strafbewehrtes) Patientenrecht
  - Bewußtsein entwickeln
- in der Praxis Güterabwägung / Verhältnismäßigkeit
  - öffentliches Interesse
  - mutmaßliches Interesse des Patienten
  - technische Möglichkeiten und Kosten
- ständig im Fluß, im Zweifelsfall:
  - zuständigen Datenschutzbeauftragten kontaktieren