Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

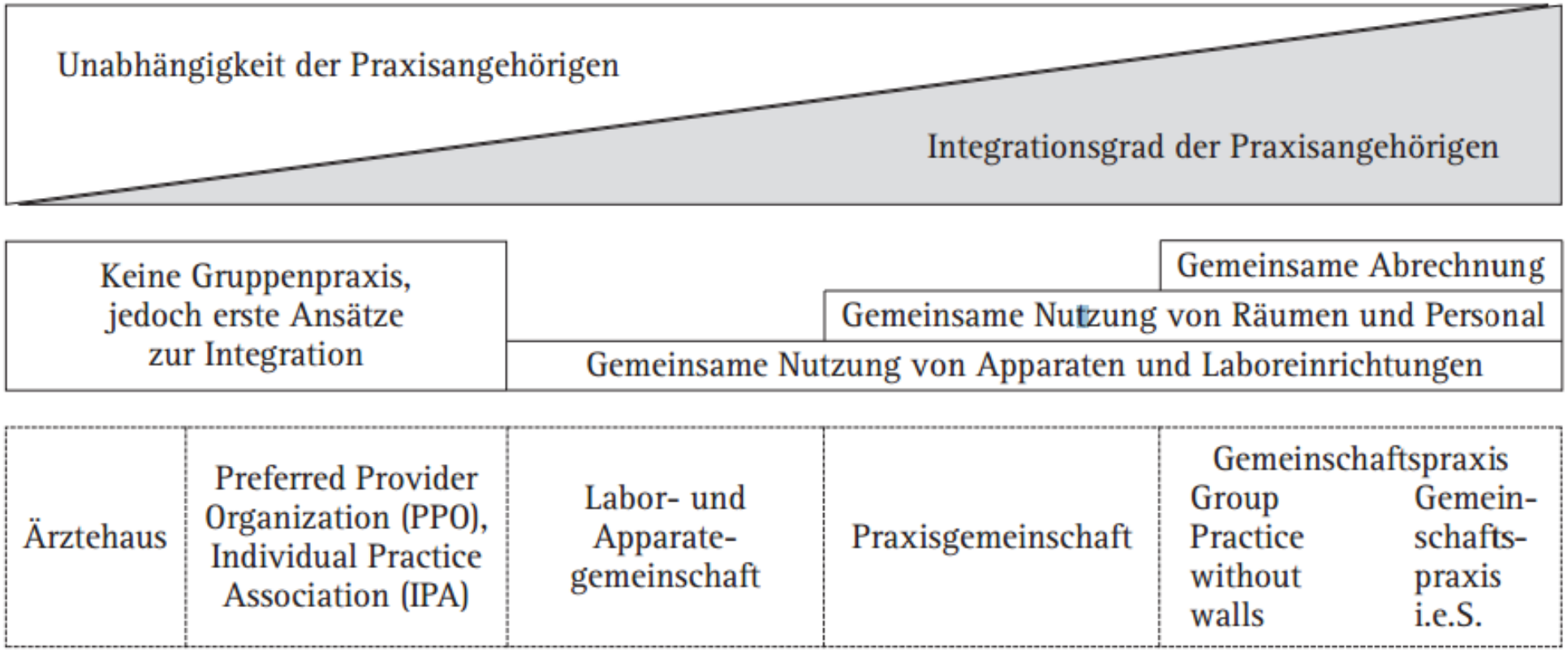
Kontrollierter Einsatz des elektronischen Patientendossiers

Günter Karjoth, Kompetenzzentrum Informationssicherheit,
Hochschule Luzern – Informatik

FH Zentralschweiz

EFQM
Recognised for excellence
5 star - 2015

Arztpraxis, Gruppenpraxis, Spital, klinische Forschungszentrum



Formen von Gruppenpraxen
Quelle: Mojon-Azzi (2001, S. 1147)

☞ vielfältiger Informationsaustausch

Besondere Anforderungen an die Sicherheitsverfahren

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Shared Workstations
- automatisches Sperren von unbesetzten Workstations
- no click access™ (Proximity Card, Fingerprint, Gesichtserkennung, ...)
- „Follow-Me" Desktop (SSO, Workflow / Applikationen)

Gesundheitsdaten sind besonders schützenswerte Personendaten

Healthcare data is unique, which makes the privacy and security of it so critical:

While credit cards can be canceled when lost or stolen, medical records can be compromised for years.

Electronic health records sell for **$50 per chart** on the black market, compared to **$1** for a stolen **social security number** or **credit card number**.[5]

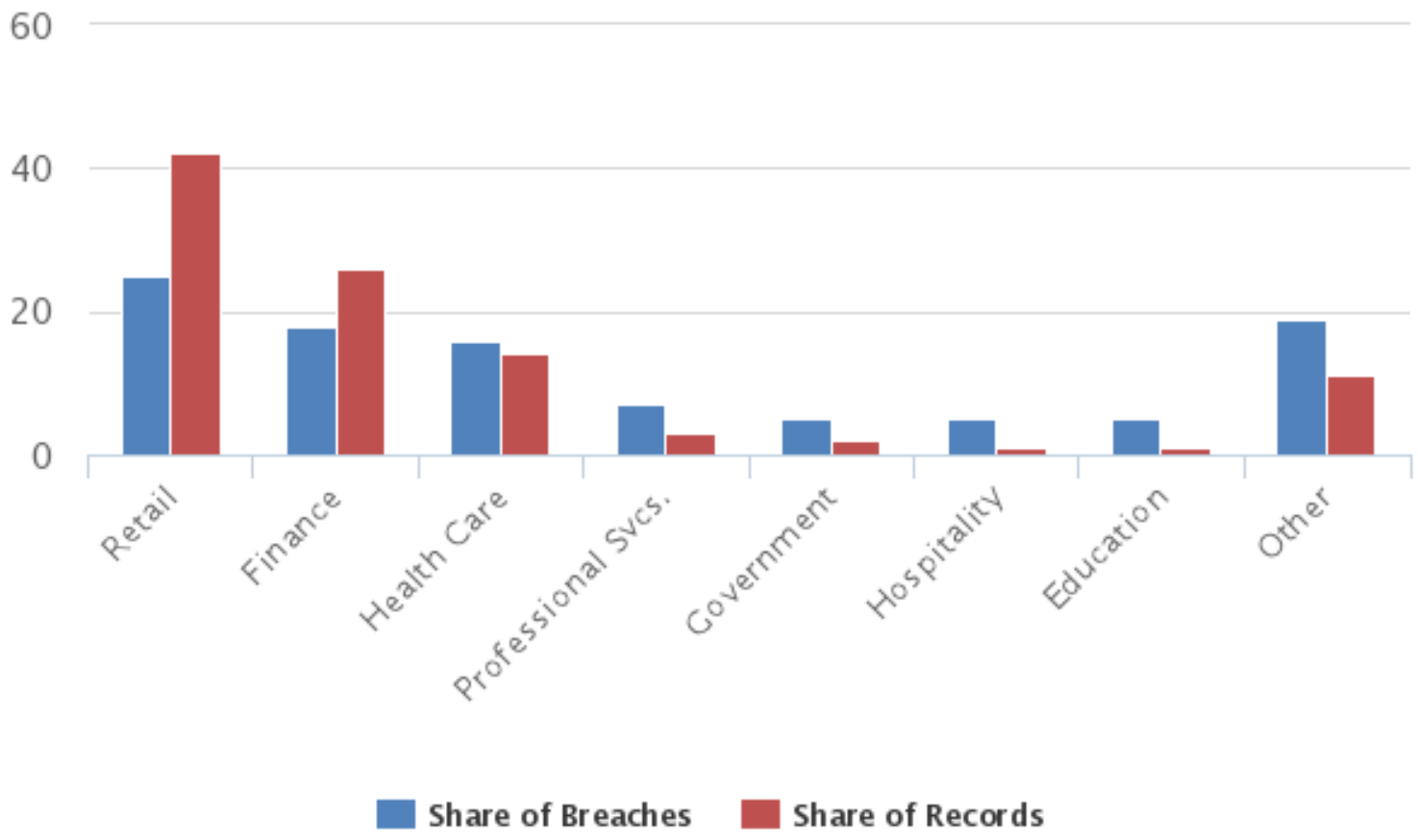
Criminal attacks, the number 1 root cause of healthcare data breaches, are rising.[6]

WHY?

Medical records contain most of the data hackers want, making them ideal for **ONE-STOP STEALING**.[7] Weak cybersecurity makes electronic protected health information (ePHI) more vulnerable.

Cybersecurity in Healthcare: Why It's Not Enough, Why It Can't Wait, Symantec, ©2016

Breaches and Records Breached Industry Sector, 2012-2015



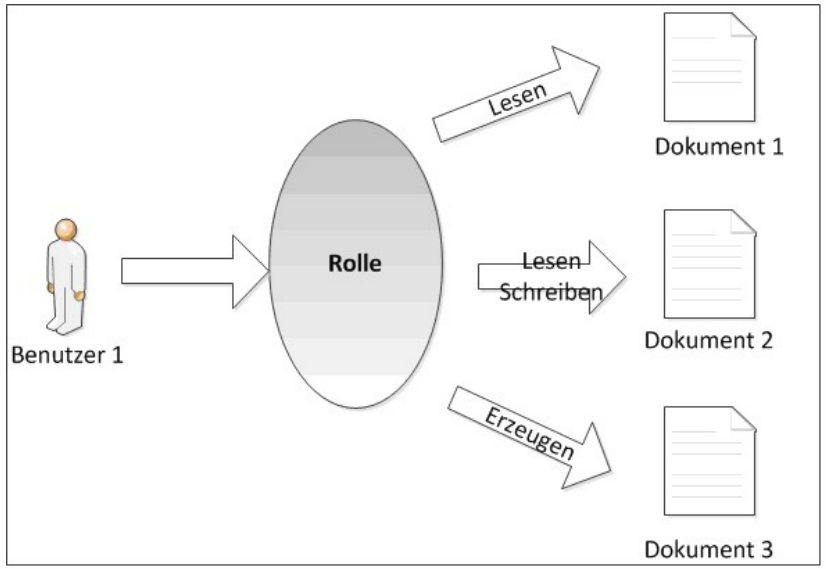
California Data Breach Report, February 2016

Rollenbasierte Zugriffskontrolle

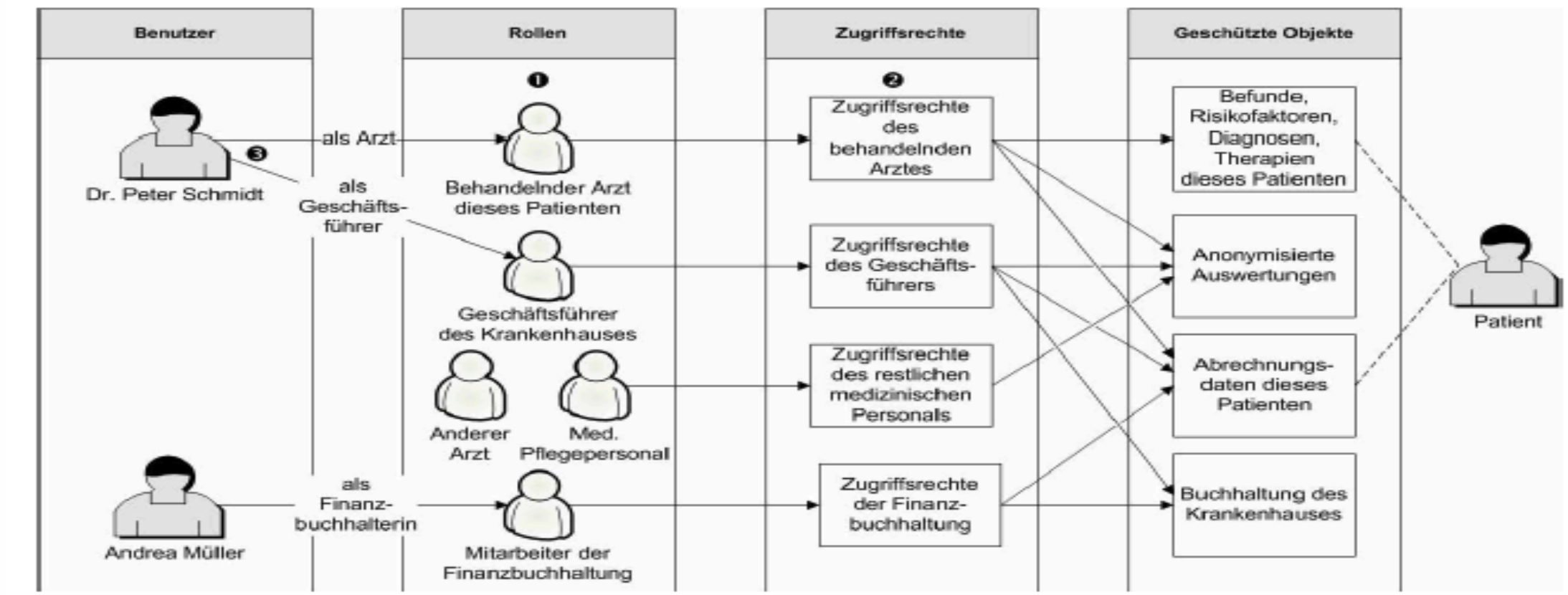
Strukturelle Rolle
- Zuständigkeit eines Mitarbeiters innerhalb einer Organisation
- über längere Zeiträume statisch

Funktionelle Rolle
- Aufgabe, die zugewiesen oder auf Grund bestehender Fachkompetenz übernommen wurde
- wechseln in Abhängigkeit vom Bezug der Tätigkeit zu der Behandlung

☞ **Bündel von Zugriffsberechtigungen**

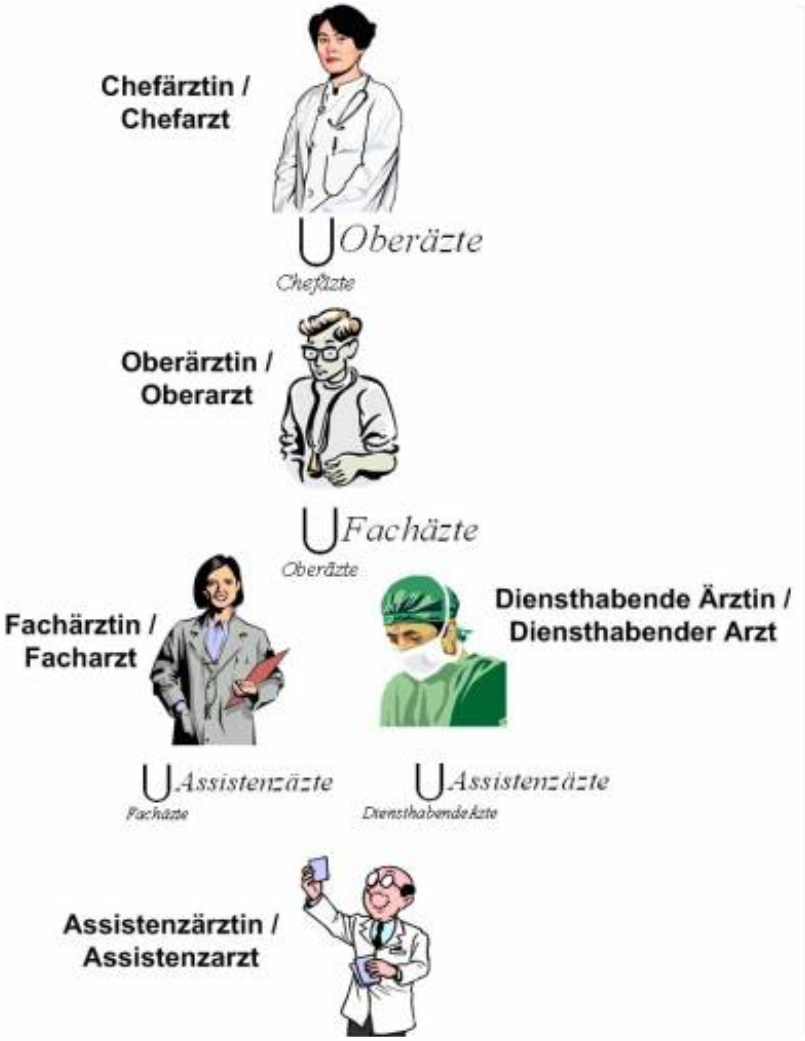


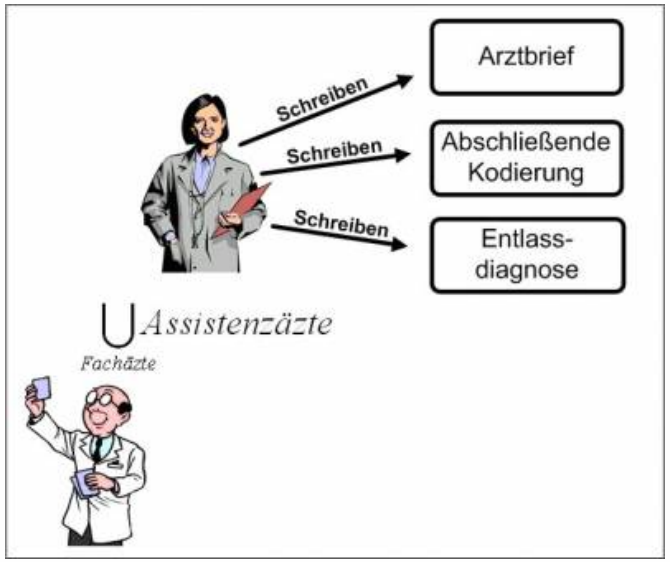
Szenario "RBAC in einem Krankenhaus"

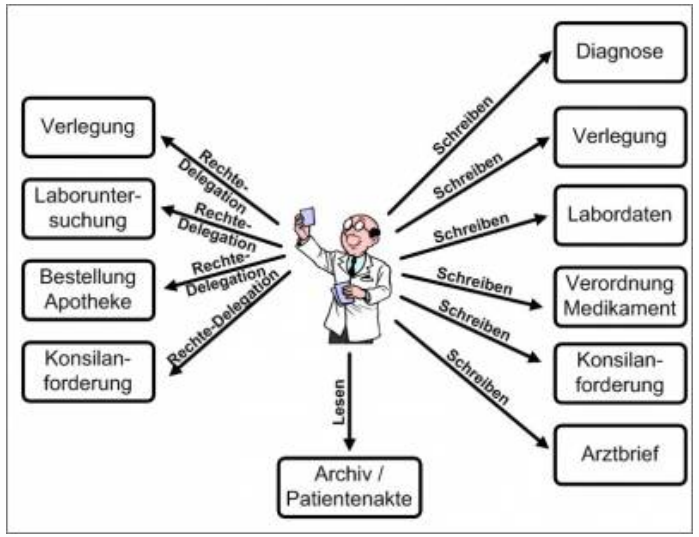


Quelle: Grimm und Meletiadou, 2007

Abstraktionen (Vererbung)

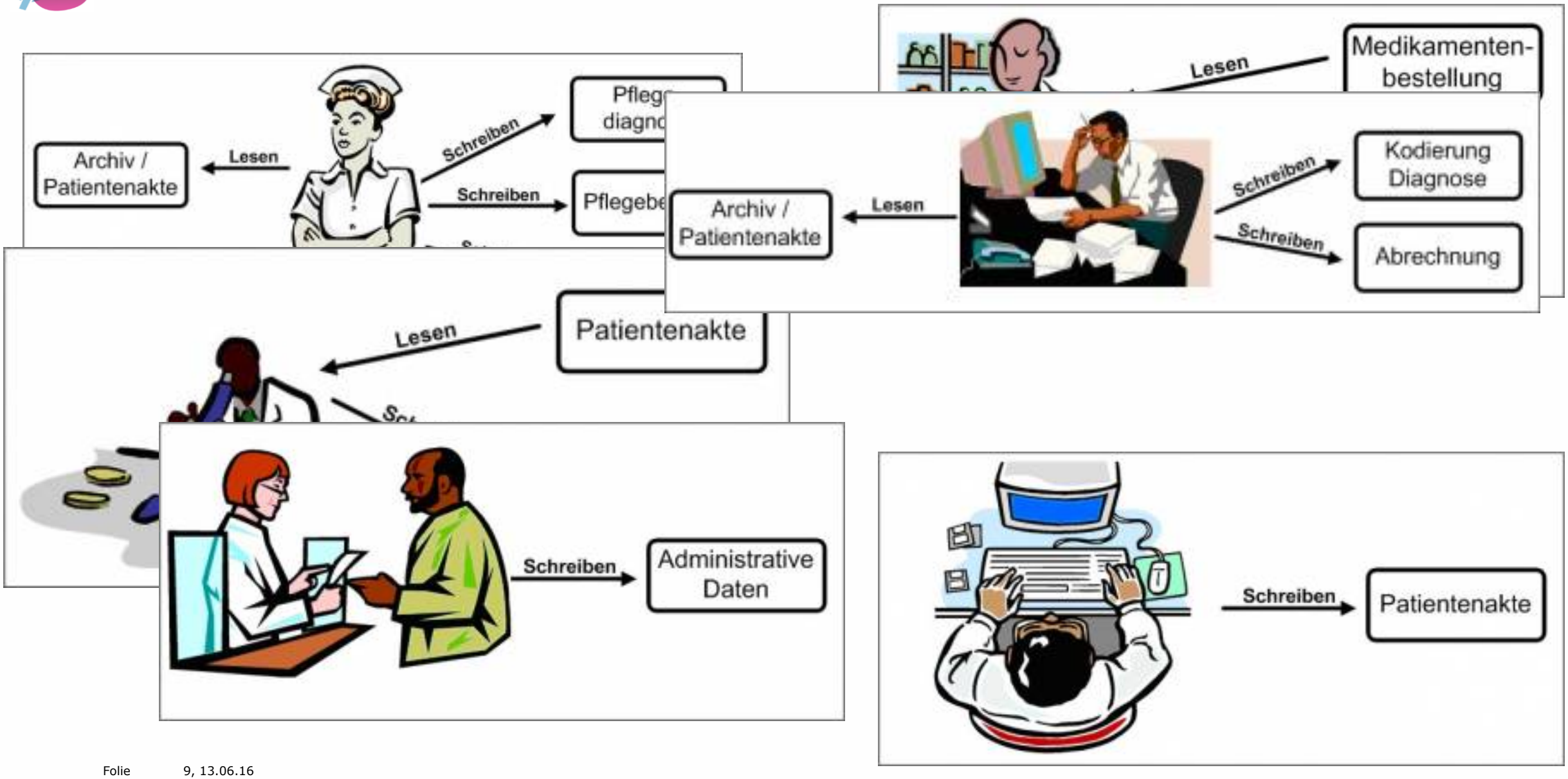






Bilderquelle: GMDS AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)

Rollenzuordnung



Bilderquelle: GMDS AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)

Beispiel Inselgruppe

- 3 Divisionen: Universitätsspital, Stadtspital und Landspitäler
- über 10‘000 Mitarbeitende
- 781‘000 ambulante Konsultationen, 61‘000 stationäre Fälle, 1‘330 Betten

- 10 Systemlandschaften mit 38 SAP Systemen
- 3’700 aktive SAP – User

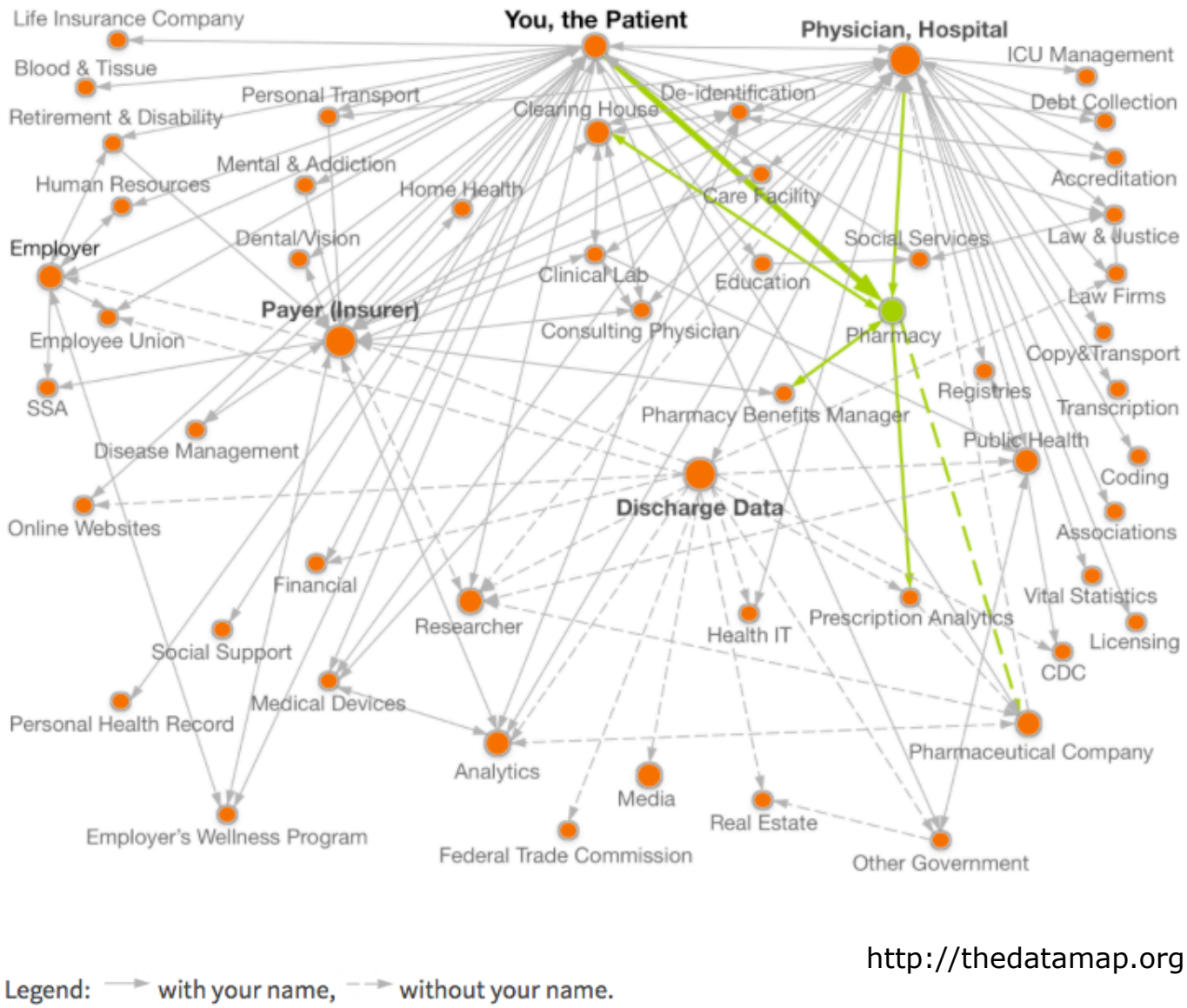
- knapp 700 Business-Rollen; je System-Landschaft rund 70 Business-Rollen
- gesamthaft rund 3’000 SAP – Sammelrollen mit vielen SAP Einzelrollen

- jede Rolle soll von mindestens zwei verantwortlichen Stellen freigegeben werden.
- rund 500 Mutationen pro Monat (stark schwankend)

☞ Berechtigungsverwaltung ist „unglaublich aufwendig“

Akteure im Gesundheitswesen

- Patient
- Versicherungen
- Ärzte
- Spitäler
- Spitex
- Apotheken
- Forschung
- Industrie
- Bundesämter
- Arbeitgeber
- …



http://thedatamap.org

ELEKTRONISCHES PATIENTENDOSSIER

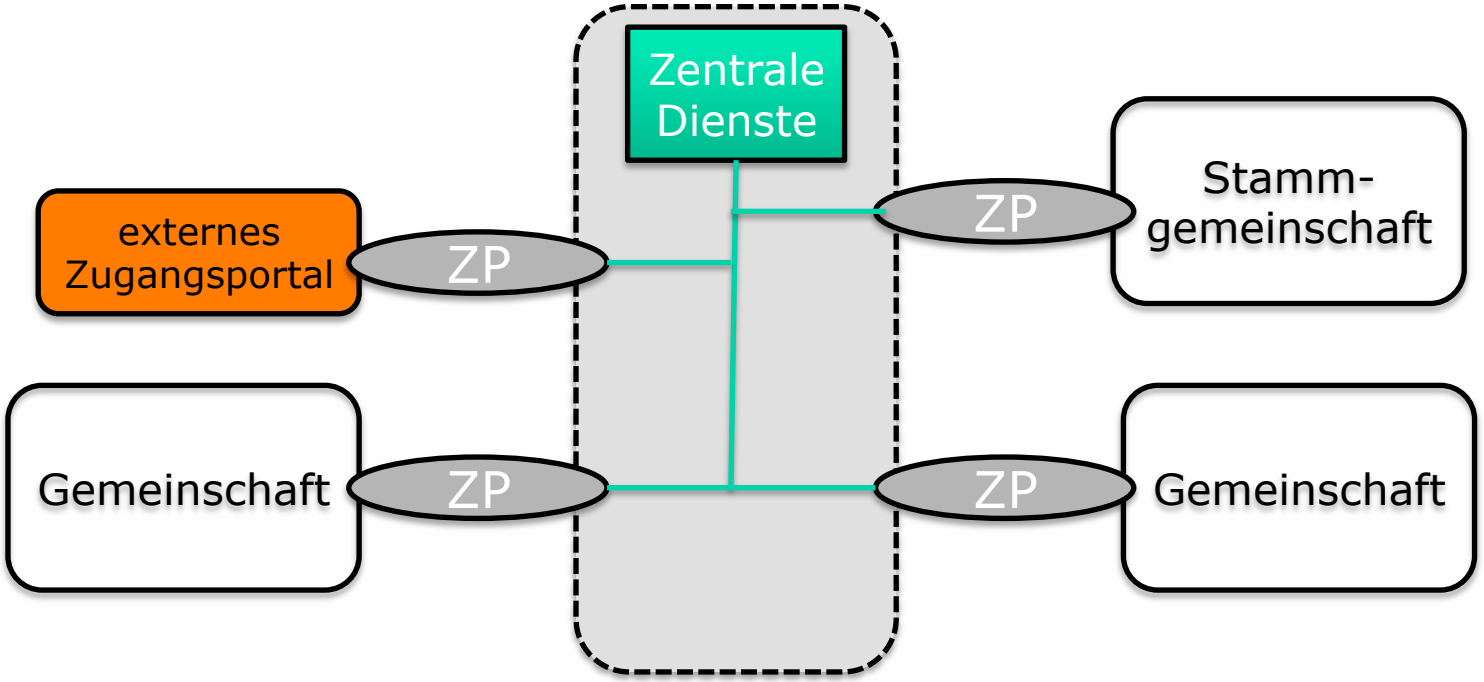
Architektur

- gleichberechtigte Gemeinschaften, die über Zugangspunkte ZP kommunizieren

- schweizweite Verzeichnisse
  - der Gemeinschaften
  - der Rollen

- Stammgemeinschaft

  - Einwilligung des Patienten, dass eine bestimmte Person in Wahrnehmung einer bestimmten Rolle Zugriff auf bestimmte Dokumente hat



☞ Der Patient / Patientin
- soll selber bestimmen können, wer welche Daten einsehen darf,
- selbst Zugriff auf ihr Dossier erhalten.

PERSONENIDENTIFIKATION

Identifikation

Daten wie Vor- und Zuname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht, Titel, Anschrift, Krankenversichertennummer, Patienten-ID.

Patientien-ID (UPI-Datenbank der Zentralenausgleichstelle)

- Patienten-Index
- Index der Behandelnden

Versichertenkarte (für Patienten)
Health Professional Card (für Gesundheitsfachpersonen) zum Verschlüsseln und Signierung von Dokumenten

☞ Single sign-on

Verzeichnisse (Zentrale Dienste)

- **Gemeinschaften und externe Zugangsportale**
  Community / Portal Index (CPI-S)

- **Behandelnden**
  Healthcare Professional Index-Service (HPI-S)
  - Beruf/Qualifikation
  - Fachrichtung
  - Berufsausübungsbewilligung (Zeitangabe/ausgebende Stelle)

- **Gesundheitsorganisationen**
  Healthcare Organisation Index-Service (HOI-S);
  - Institutionen, Organisationen, virtuelle Gruppen

- **Rollen**
  Rollen Index-Service (RI-S)

- **Dokumenten-Metadaten**
  Metadaten Index-Service (MDI-S).

Zugang zum ePD

Grundsätzlich gilt, dass nur Personen das ePD einsehen können, denen der Patient ein Zugriffsrecht erteilt hat.

- Zugriff auf einzelnes Dokument abhängig von dessen zugewiesener Zugriffs- und Vertraulichkeitsstufe

- Patientenadministratoren haben nur Zugriff auf die demographischen Daten

- Im Alltag kann es vorkommen, dass Praxisassistenten, Apothekerhelfer (Hilfspersonen) unter der Verantwortung ihrer vorgesetzten Gesundheitsfachperson auf das ePD zugreifen ☞ Delegation

- Mitglieder einer zertifizierten Gemeinschaft oder Stammgemeinschaft (Gesundheitsfachpersonen und deren Einrichtungen)

- Haftet die (Stamm)Gemeinschaft bei Datenmissbrauch?

Komplexität

- IT-Infrastruktur für den sicheren Datenaustausch

- Ablage Dokumente
- Register Dokumente

- Berechtigungssystem

- Zugangsportal

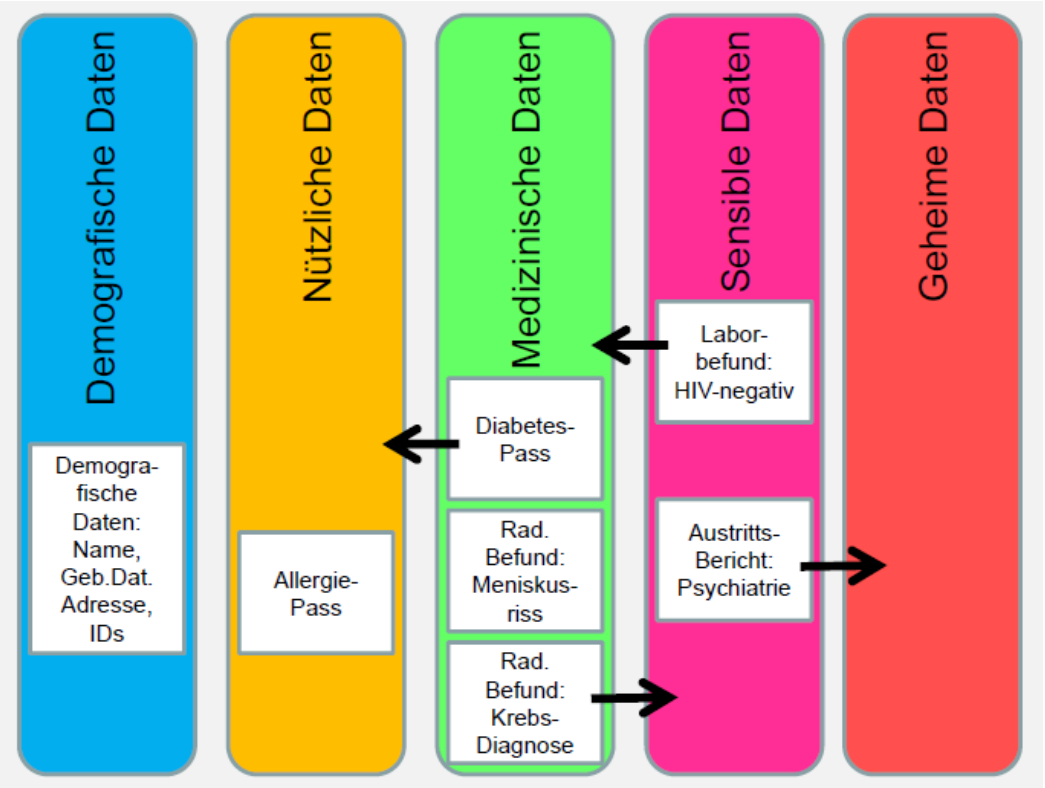
☞ zertifizierte Komponenten

BERECHTIGUNGSSYSTEM

Zugriffssteuerung: Rechtematrix

Vertraulichkeitsstufen

*



Zugriffsstufen

- administrativ *
- eingeschränkt (Behandelnde allgemein)
- normal (Mein Behandelnder)
- erweitert (Mein Behandelnder des Vertrauens)
- Notfall
- gesamt → Patient vorbehalten

★ In der EPDV gibt es die Stufen „Demographische Daten" und „administrativ" nicht mehr!

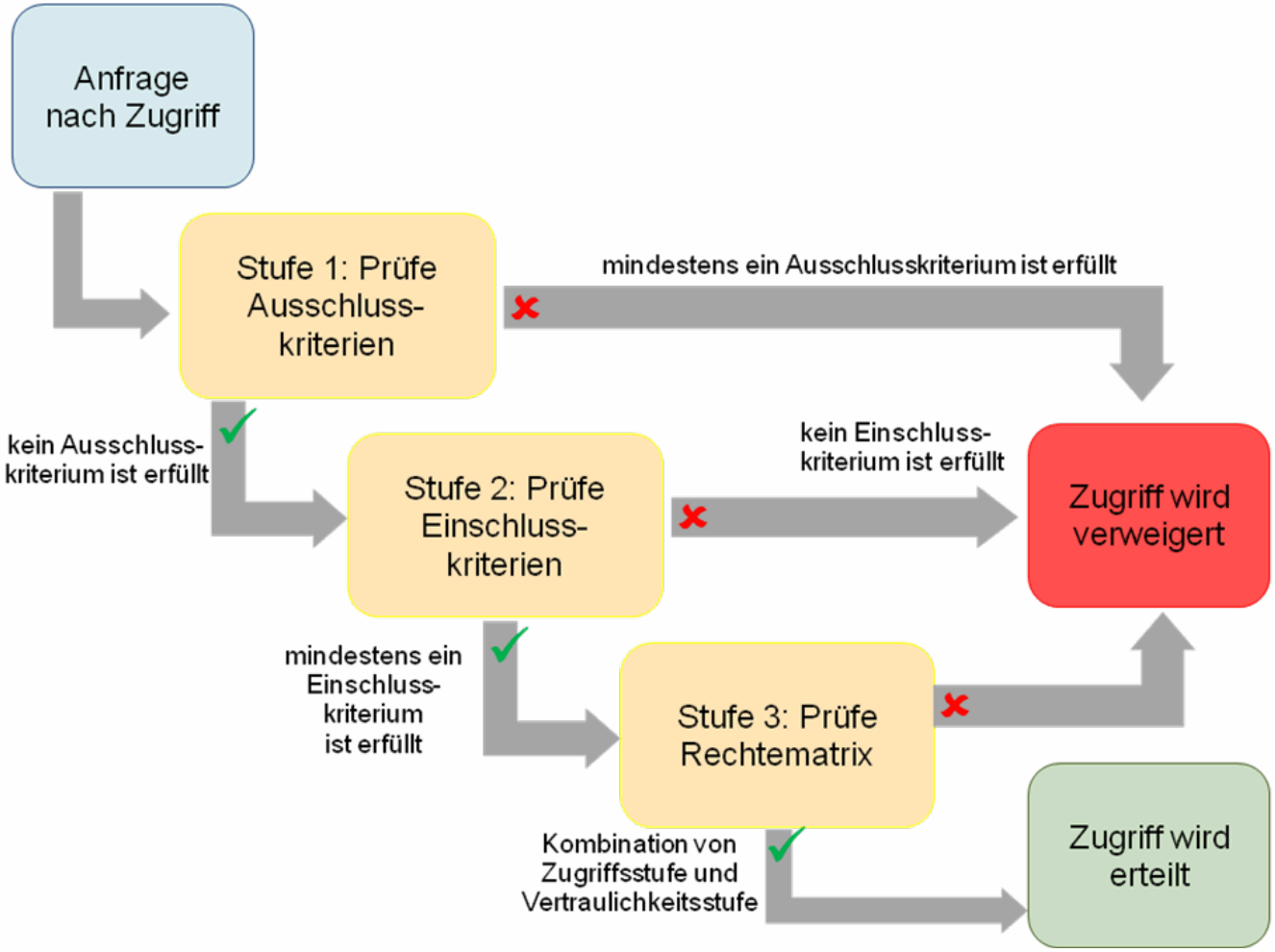
Quelle: eHealth Suisse: Standards und Architektur: Empfehlungen V, 2014

Grundeinstellung

		Vertraulichkeitsstufen						
		Demografische Daten	Nützliche Daten	Medizinische Daten	Sensible Daten	Geheime Daten		
EPD-Akteure	Patienten-administrator	✓/✗	✗	✗	✗	✗	Zugriffsstufe „administrativ“	Zugriffsstufen
	Gesundheits-fachperson mit Behandlungs-kontext	✓/✗	✓/✗	✗	✗	✗	Zugriffsstufe „eingeschränkt“	
		✓	✓	✓	✗	✗	Zugriffsstufe „normal“	
		✓	✓	✓	✓	✗	Zugriffsstufe „erweitert“	
		✓	✓	✓	✗/✓	✗	Zugriffsstufe „Notfall“	
	Patient	✓	✓	✓	✓	✓	Zugriffsstufe „gesamt“	

✓/✗ = Grundeinstellung ist ja ✗/✓ = Grundeinstellung ist nein

Dreistufiges Regelwerk



☞ Die Ausschlussliste übersteuert alle anderen Regeln!

Einwilligung, informierte (EPD)

Schriftliche Einverständniserklärung des Patienten, der vorgängig angemessen informiert wurde, um ein elektronisches Patientendossier zu eröffnen.

Umfassende Aufklärung des Patienten
- Zweck und Regeln des EPD verstanden und abschätzen können
- in welche Datenbearbeitungen sie einwilligen
- Verweis auf die gesetzlichen Grundlagen

Was bedeutet die Einwilligung für den Patienten/die Patientin:
- Beschreibung
    - der Daten, die zwischen den Gesundheitsfachpersonen ausgetauscht werden sollen;
    - des Personenkreises, der auf diese Daten Zugriff haben kann.
- Auswirkung auf die Behandlung des Patienten und auf den Informationsaustausch;

☞ Einwilligung wird in bestimmten Fällen vermutet.

☞ Patient muss genügend aufgeklärt sein über die Auswirkungen seiner Handlungen bei der Verwaltung seiner Rechteattribute.

Sonderzugriffe

- **Notfall**
  Sie gehen über die beschränkte Rollen- und Aufgaben-bezogene Berechtigung zum Zugriff auf Patientendaten hinaus.

- **Vertretung**
  zeitlich befristete Übernahme der Aufgabe eines Mitarbeiters durch einen anderen, die von der jeweilig dafür zuständigen Leitung im Voraus festgelegt wurde.

☞ Stellvertretung des Behandelnden (Abwesenheit / Urlaub) muss explizit vom Patienten ermächtigt werden.

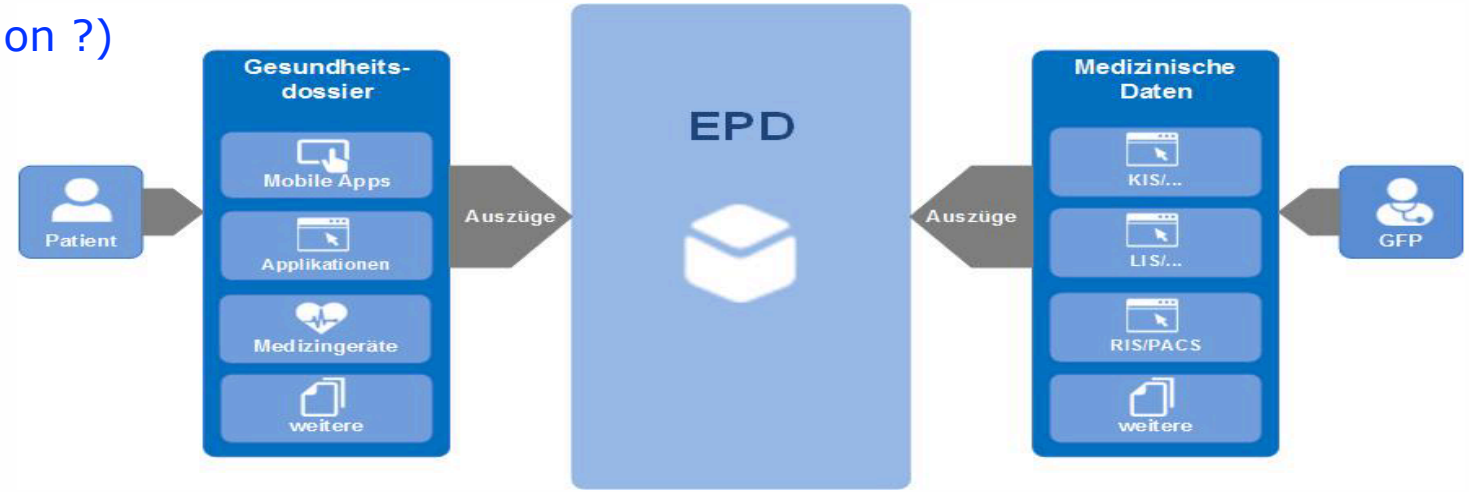
- **Ermächtigung**
  Patient kann das Recht auf Zuweisung einer Zugriffsstufe an eine GFP stellvertretend auch seinen Behandelnden geben.
  - nur GFP seiner Stammgemeinschaft kann dieses Recht erhalten
  - die neu zugriffsberechtigten GFPs können auch in anderen Stammgemeinschaften sein

Patientenseitige Daten im EPD

- im EPD sind nur IHE-konforme Dokumente zugelassen

- publizieren eines Dokumentes über das interne Zugangsportal der Stammgemeinschaft
  - übersieht Erfassung der Metadaten (z.B. Titel, Erfassungsdatum)
  - Eintrag ins Registry
  - Speicherung im Dokumenten–Repository
  - Verwaltung der Zugriffsrechte

☞ Patient ist „Dokumenten-Quelle" wie andere GFP auch, aber
  - Validierung durch eine GFP
  - Wechsel der Stammgemeinschaft
  - Daten sind in der Cloud (Authentifikation ?)



Quelle: Konzept "Patientenseitige Daten im EPD", HINT AG

Fazit

- Integration in bestehende Informationssysteme

- Vielzahl von Akteuren
  - sichere Authentifikation / Registrierung

- komplexes Rechtesystem
  - positive & negative Rechte, zeitliche Beschränkung
  - Rollen und Gruppen
    - wer definiert Gruppen ?
  - Schreibrecht
    - implizite Zustimmung bei Eröffnung eines EPD
    - Schreibrecht ohne Leserecht ?
  - Müssen Voreinstellungen zertifiziert werden? Gegen was?
  - Stellvertreterregelung (GFP / Eltern / Vormund)

- Governance und Accountability
  - Zertifizierung