# Datenschutzfragen zur Telemedizin

## Grundlagen, Entwicklungsstand, Aussichten

**Datenschutz in der Medizin - Update 2015**

**Hamburg, 03.02.2015**

**Dr. Georgios Raptis**
**Bundesärztekammer**

# Inhalt und Abgrenzung

- Inhalt des Vortrags
  - Technischer Datenschutz und Empfehlungen zur IT-Sicherheit in telemedizinischen Szenarien
- Abgrenzung
  - Keine Aussagen zur berufsrechtlichen oder sonstigen rechtlichen Zulässigkeit bestimmter telemedizinischer Szenarien
  - Keine Aussagen, unter welchen medizinischen oder rechtlichen Voraussetzungen bestimmte telemedizinische Szenarien möglich oder sinnvoll sind
  - Keine juristischen Aussagen oder Empfehlungen

# Datenschutz/Telemedizin Grundlagen

**Für Telemedizinische Anwendungen gelten dieselben datenschutzrechtlichen Grundsätze wie auch sonst in der Medizin**

- Z.B. § 203 StGB, BDSG, Landesdatenschutzgesetze
- Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit von Patientendaten müssen effektiv geschützt werden

- **wie?**

# Definition Telemedizin

## Definition Telemedizin:

*Telemedizin ist ein Sammelbegriff für verschiedenartige ärztliche Versorgungskonzepte, die als Gemeinsamkeit den prinzipiellen Ansatz aufweisen, dass medizinische Leistungen der Gesundheitsversorgung der Bevölkerung in den Bereichen* ***Diagnostik****,* ***Therapie*** *und* ***Rehabilitation*** *sowie bei der ärztlichen* ***Entscheidungsberatung*** *über* ***räumliche Entfernungen*** *(oder* ***zeitlichen Versatz****) hinweg erbracht werden. Hierbei werden Informations- und Kommunikationstechnologien eingesetzt*

## Datenschutz: Wo und Wann muss man die Daten schützen? Wie?

→ Informationsfluss bei Telemedizin analysieren, Ansatzpunkte finden

# Informationsfluss bei Telemedizin

- Austausch von Informationen
  - Über ***räumliche Entfernungen***
    - Datenübertragung
    - dabei (flüchtige) Speicherung in zwischengeschalteten Systemen
  - Evtl. mit ***zeitlichem Versatz***
    - (Datenübertragung)
    - Mittel- bis langfristige Speicherung in zwischengeschalteten Systemen

# Informationsfluss bei Telemedizin

- Austausch von Informationen

## → Datenübertragung

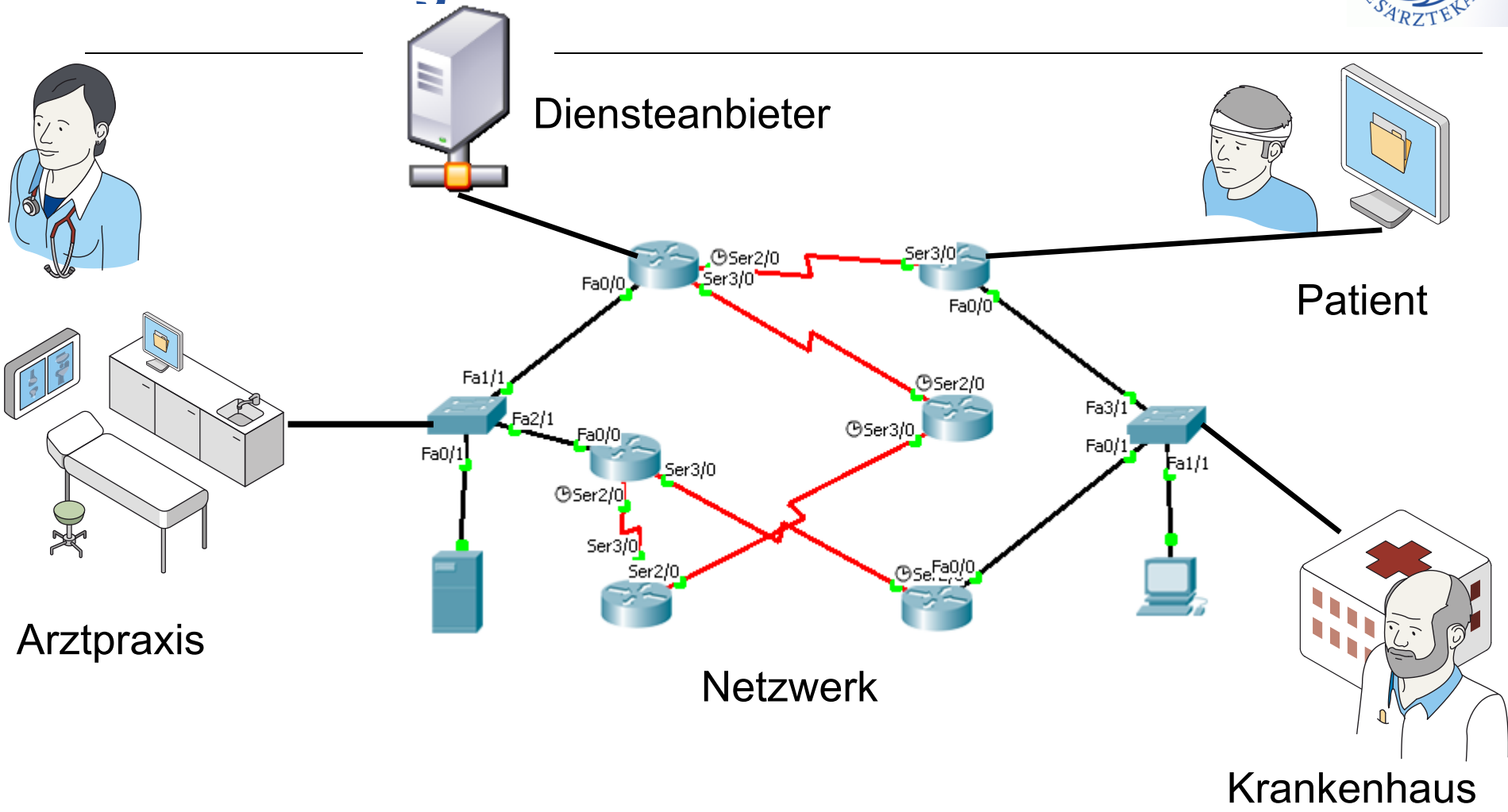
- Zwischen Ärzten, ggf. weiteren Gesundheitsfachberufen
  - (Arzt)praxis, Krankenhaus, spezialisiertes Zentrum, mobiles Gerät
- Zwischen Arzt und Patient
  - (Arzt)praxis, Krankenhaus, spezialisiertes Zentrum, mobiles Gerät ←→ Patient

# Informationsfluss bei Telemedizin

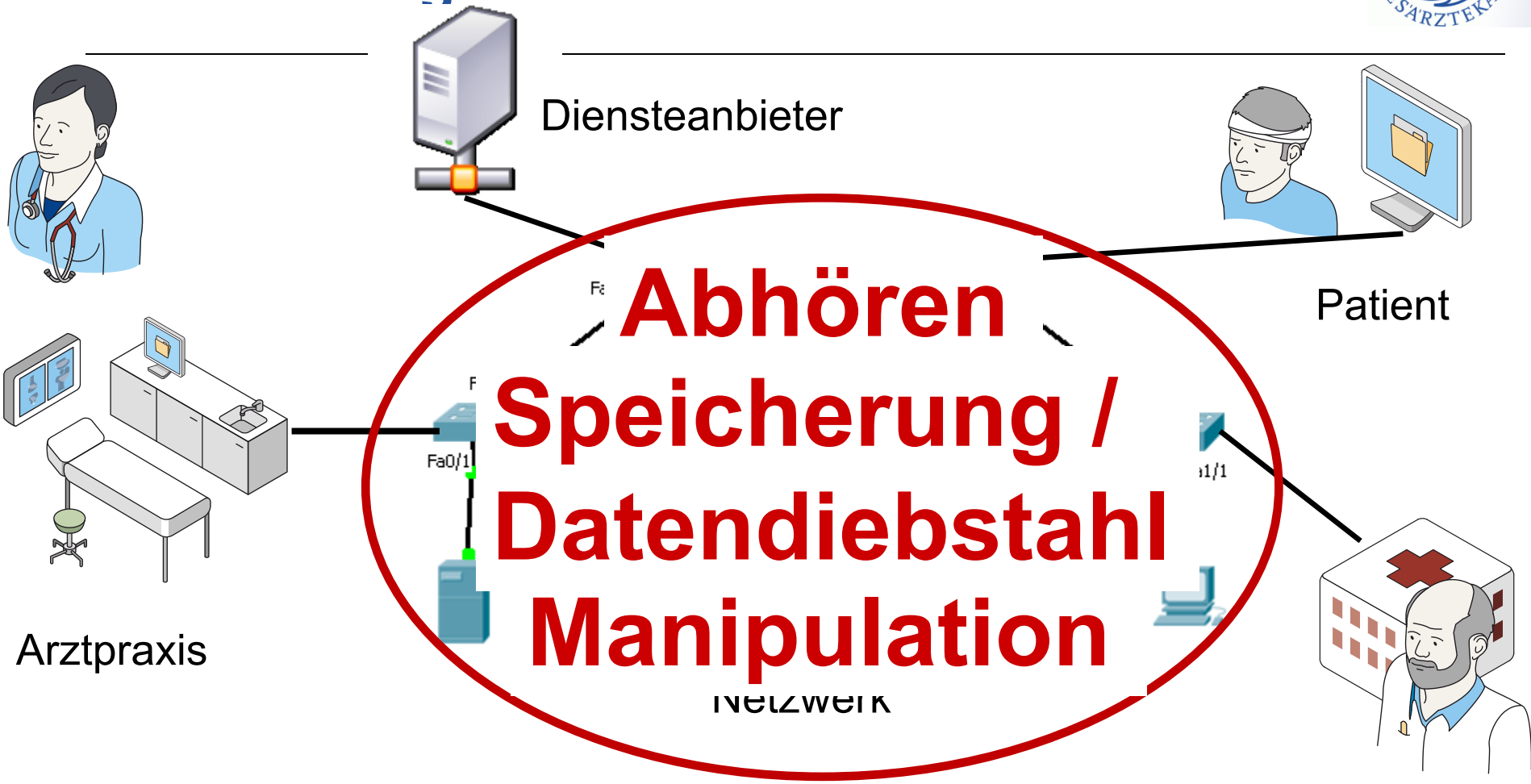
- **Speicherung** von Informationen
  - Flüchtige Speicherung bei der **Datenübertragung**
    - Infrastrukturanbieter (z.B. Telefon-/Internetprovider, Mobilfunkanbieter, Safenet, Telematik-Infrastruktur)
  - Mittel- bis langfristige **Speicherung** (bei „zeitlichem Versatz“)
    - Spezialisierte Diensteanbieter („Medizinische Clouds“, Telemedizin-Zentren, Krankenhäuser, künftige Dienste der Telematik-Infrastruktur)

**→ Sicherheitstechnisch nur minimaler Unterschied**

# Betrachtung Informationsfluss



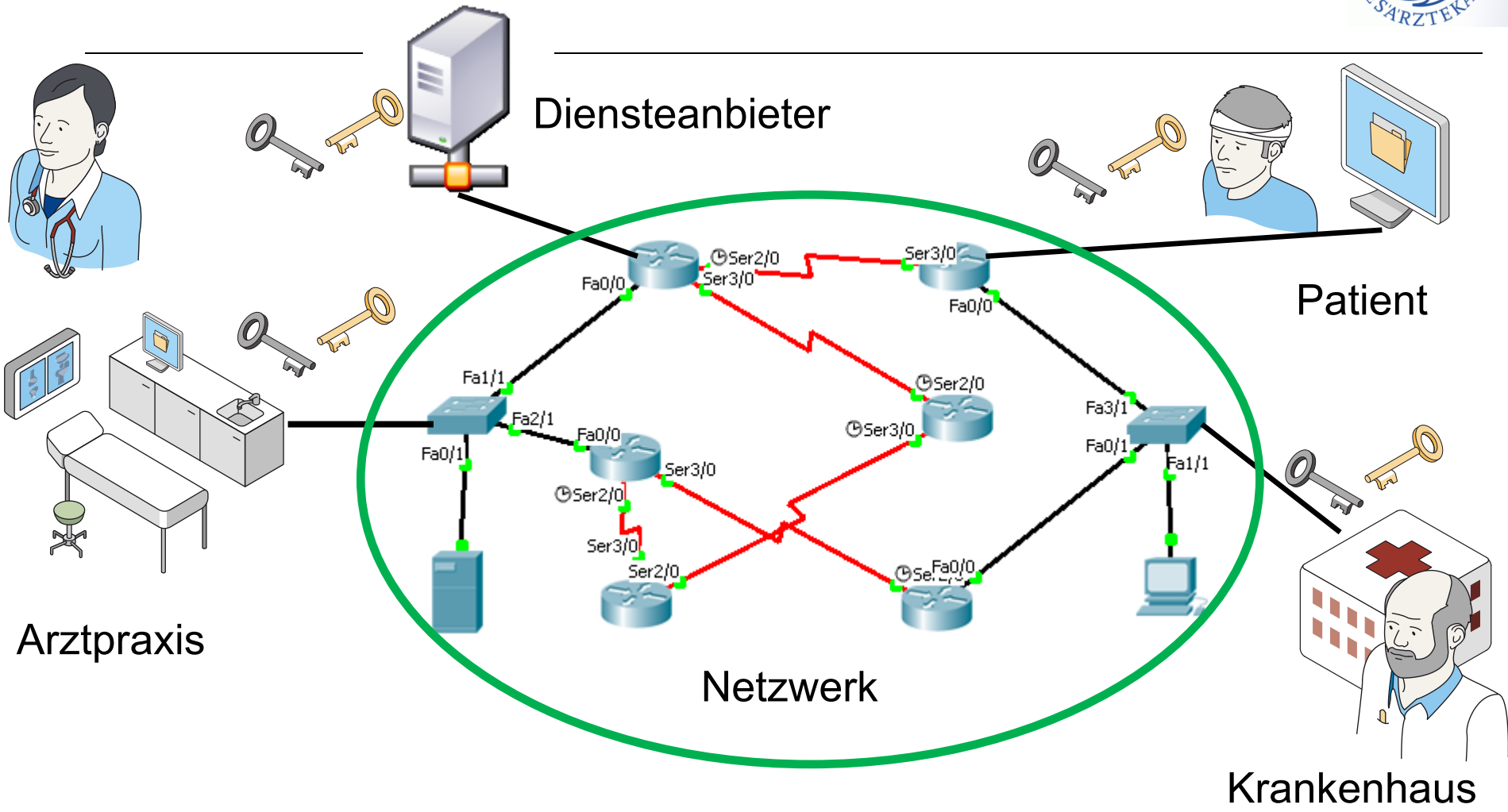
# Betrachtung Informationsfluss




## Fokus auf technischen Datenschutz:

- **Übertragungsweg**

# Erste Erkenntnisse




## Schutz der Daten beim Übertragungsweg

- ***Ende-zu-Ende* Verschlüsselung**

# Anforderungen Übertragungsweg

## Verschlüsselung aller Daten

- *Ende-zu-Ende*, d.h. Daten werden bereits beim Absender verschlüsselt und können nur beim Empfänger wieder entschlüsselt werden
  - Schutz gegen Abhören
  - Schutz gegen unbefugter Speicherung während der Übertragung
  - So kann auch die Speicherung von medizinischen Daten, z.B. als ePatientenakte in einem Dienst abgesichert werden

# Verschlüsselung: Ist das sicher?

E. Snowden, 2013: „**Encryption works**. Properly implemented strong crypto systems are one of the few things that you can rely on“

$n=p*q$, $\varphi(n)=(p-1)(q-1)$, $\gcd(\varphi(n),e)=1$,
$d*e=1 \bmod \varphi(n)$,
$C=M^e \bmod n$, $M=C^d \bmod n$

„Edward Snowden-2“ von Laura Poitras / Praxis Films
- Screenshot of the film Prism by Praxis Films

- Bitte **sichere und effektive Kryptographie** benutzen!
- Bitte **sichere Schlüssel** verwenden! Z.B. in einer zertifizierten Chipkarte (eArztausweis)

# Anforderungen für Telemedizin-Projekte

- Entweder selbst für eine gute Verschlüsselung sorgen,
- oder diese Funktionalität bei einem spezialisierten Anbieter einkaufen
  - Mit entsprechenden Zusicherungen und Sicherheitszertifizierungen für die Komponenten
  - → Technische Details für eine sichere Verschlüsselung in der jeweils aktuellen Technischen Richtlinie BSI-TR-03116-1 des BSI
- oder geeignete Funktionen und Komponenten der Telematik-Infrastruktur nutzen, sobald verfügbar
  - Sicherheitszertifizierungen und starke Verschlüsselung sind Voraussetzungen für den Einsatz von Diensten und Komponenten in der Telematik-Infrastruktur

# Verschlüsselung: Ausreichend?

E. Snowden, 2013: „**Encryption works**. Properly implemented strong crypto systems are one of the few things that you can rely on…“

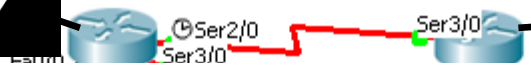
„Edward Snowden-2“ von Laura Poitras / Praxis Films
- Screenshot of the film Prism by Praxis Films

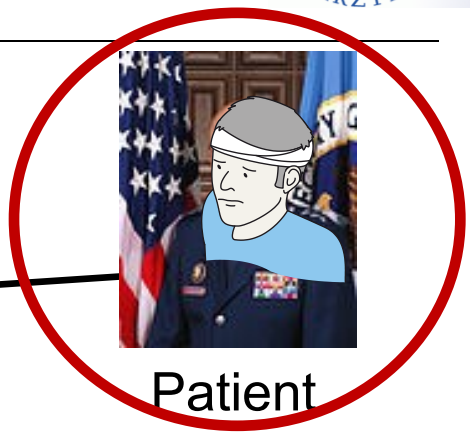
**„…Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it“**

- Bitte **sichere Komponenten** für die Verschlüsselung und den Schutz der eigenen IT verwenden!
  Z.B. mit Sicherheitszertifizierung

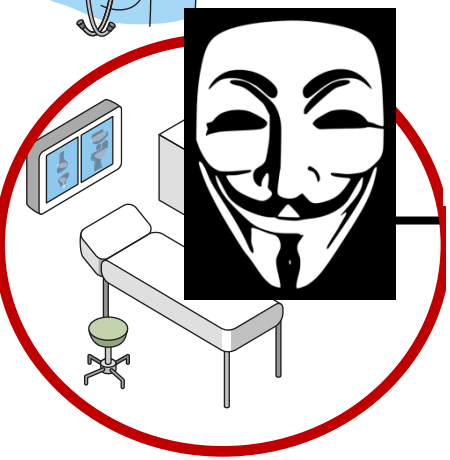
# Betrachtung Informationsfluss

steanbieter



Patient



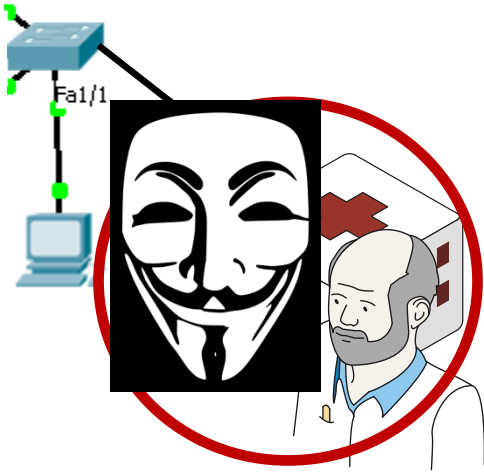
Arztpraxis

**Falsche Identität**

**Datendiebstahl**

**(„Hacken“)**

**Manipulation**

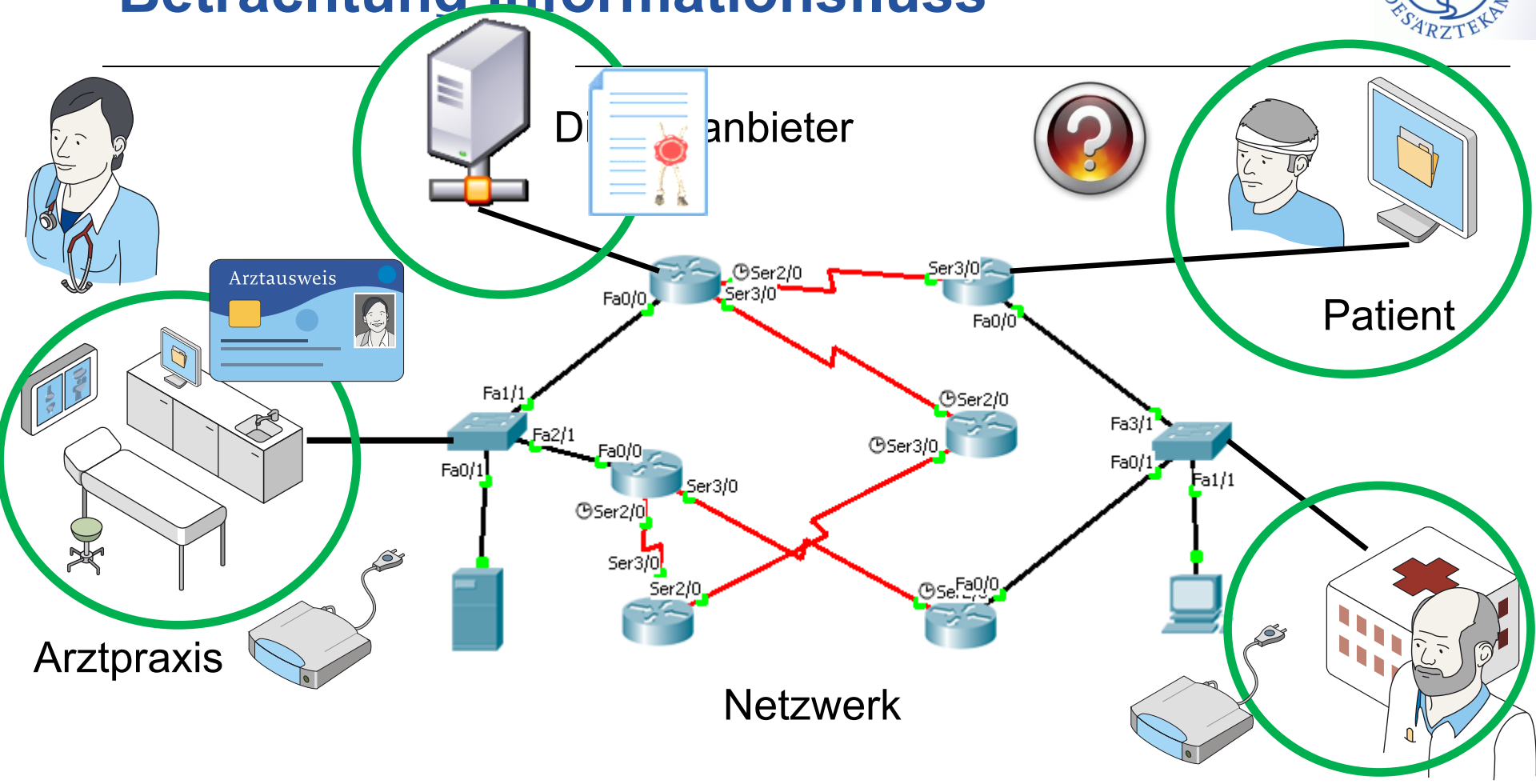



Krankenhaus

## Fokus auf technischen Datenschutz:

- **Endpunkte der Kommunikation**

# Betrachtung Informationsfluss




## Schutz bei den Endpunkten der Kommunikation:

- **Authentifizierung**
- **Sichere Komponenten: VPN / Firewall**

# Anforderungen Arztpraxis / Krankenhaus

## Authentifizierung (Ist es wirklich der Arzt?)


- Z.B. mit Hilfe des eArztausweises
- Z.B. mit Hilfe von Zugangsdaten, die von einem Telemedizin-Dienst geprüft werden
  - Username/Passwort für den Arzt: nicht ausreichend sicher!
  - 2-Faktor- oder kryptographische Verfahren notwendig
- Ausnahme: bei telemedizinischen Diensten mit Video-Konsultation ist eine elektronische Authentifizierung zweitrangig
  - Man sieht ja den Arzt und kann ihn persönlich erkennen…

# Anforderungen Arztpraxis / Krankenhaus

## Schutz der eigenen IT-Infrastruktur:

## → sichere Komponenten

- Firewall, aktuelles Betriebssystem und Antivirus-Software
- Trennung von Patientendaten führenden Systemen und Internet
  - **Hardware VPN-Device**
    - Konnektor oder Safenet-Gerät
  - „Einwahl“ in einem abgesicherten, privaten Netz
  - Krankenhaus / Telemedizin-Zentrum: Absicherung durch professionelle IT-Sicherheitsmaßnahmen und Komponenten
  - Abgesicherter, isolierter Rechner?

# Anforderungen Arztpraxis / Krankenhaus

## Telemedizin-Komponente der Praxis

- Denkbares Szenario:
  - Praxis-IT hat keine Verbindung ins Internet
  - Telemedizin über einen dedizierten „Telemedizin-Rechner“, der von einem Telemedizin-Anbieter bereitgestellt und gewartet wird
  - Anbieter ist verantwortlich für die Sicherheit des Systems
- **Machbar**, aber Aufwand und Verantwortung, um die Sicherheit zu gewährleisten
- → Für einen Anbieter ist es einfacher, auf ein bereits existentes, nachweisbar sicheres Netz aufzusetzen
  - z.B. Safenet oder die Telematik-Infrastruktur (wenn verfügbar)

# Telemedizin über ein geschlossenes System

## Absicherung der Patienten-IT?

- Wenn fertig konfigurierte telemedizinische Komponenten vom Arzt oder von einem Telemedizin-Anbieter dem Patienten bereitgestellt werden, **müssen diese entsprechend sicher sein**
  - Telemedizinisches System als geschlossenes Gesamtsystem, Patientenkomponente ist ein Teil davon
  - Beispiel: online-fähiges EKG-Gerät und Waage zur Telemonitoring bei Herzinsuffizienz-Patienten, bereitgestellt durch Krankenhaus

# Telemedizinische Leistungen über offene Systeme

## Kommunikation erfolgt über IT-Infrastruktur des Patienten

- Video-Sprechstunde, über eine Webseite allgemein verfügbar
- Angebot des Arztes für eine (verschlüsselte) E-Mail-Kommunikation
- Webportal mit Möglichkeit der Kommunikation
  - Patient kann Textnachrichten, Fotos/Videos, RR-/Blutzuckerwerte usw. dem Arzt bereitstellen
  - Arzt kann ggf. live antworten

→ Analogie mit telefonischer Kommunikation

# Telemedizinische Leistungen über offene Systeme

## Kommunikation mit den Patienten über „Internet-Rechner“ der Praxis?

- Denkbares Szenario:
  - Praxis-IT hat keine Verbindung ins Internet
  - Kommunikation mit Patienten (z.B. Video-Sprechstunde, Chat, verschlüsselte E-Mail) über einen dedizierten „Internet-Rechner“
  - Ist das OK?

# Telemedizinische Leistungen über offene Systeme

## Kommunikation mit den Patienten über „Internet-Rechner“ der Praxis?

→ **Ja**, mit einem gut gesicherten („gehärteten“) Rechner wäre dies OK

- Am Besten diesen Rechner von einem kompetenten IT-Dienstleister absichern („härten“) und warten lassen
- Besser wäre jedoch die Kommunikation über ein gesichertes Netz
  - Über Konnektor in die Telematikinfrastruktur (wenn verfügbar) → Sicherheitsgateway → Patient
  - Über Safenet, falls möglich

# Sonderfall telemedizinische Leistungen über ein offenes System

## Absicherung der Patienten-IT: Sache des Arztes?

- Bei Nutzung eines offenen Systems muss der Patient für die Sicherheit der eigenen IT sorgen
- Der Arzt muss den Patienten darauf hinweisen!
- Der Arzt muss **die Möglichkeit** für eine sichere Kommunikation anbieten
  - Zertifikate/Schlüssel für verschlüsselte E-Mail
  - Video-Kommunikation oder Web-Portal mit Ende-zu-Ende Verschlüsselung
- Nutzung muss für den Patienten freiwillig sein

# Die Antwort auf alle Fragen

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis,

inkl. Addendum zur Technischen Anlage (2014)

- Dtsch Arztebl 2014; 111(21): A-963 / B-819 / C-775

→ http://www.aerzteblatt.de/pdf.asp?id=160315

Technische Anlage (2008)

- Dtsch Arztebl 2008; 105(19): A-1026 / B-890 / C-870

→ http://www.aerzteblatt.de/down.asp?id=2316

# Danke für Ihre Aufmerksamkeit!


Dr. med. Dipl.-Inform. Georgios Raptis
Referent IT-Sicherheit in der Medizin
Dezernat Telemedizin und Telematik
Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

Georgios.Raptis@baek.de