



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik



Datenschutz und Datensicherheit im EPDG

Nicolai Lütschg, Projektleiter EPDG

Information Security in Health
Conference



Der Auftrag des BAG

«Das BAG setzt sich kompetent für die Gesundheit ein, fördert eine gesunde Lebensweise und sorgt dafür, dass es den Menschen in unserem Land gut geht.

Das BAG ist verantwortlich dafür, dass unser Gesundheitssystem leistungsfähig und bezahlbar bleibt.»



Rollenteilung im Gesundheitssystem

Bund und Kantone teilen sich die Kompetenzen.

Bund und Kantone sind Partner:

- bei der Erarbeitung von Strategien und Vorschriften,
- bei der Aufsicht über das Gesundheitssystem.

Zuständigkeiten Bund

- Gesundheitspolitik
- Nationale Gesetzgebung
- Interessenvertretung im Ausland

Zuständigkeiten Kantone

- Medizinische Versorgung
- Vollzug der Bundesgesetze
- Kantonale Gesetzgebung

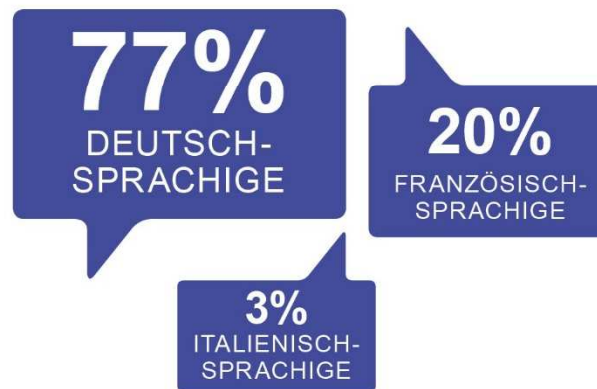
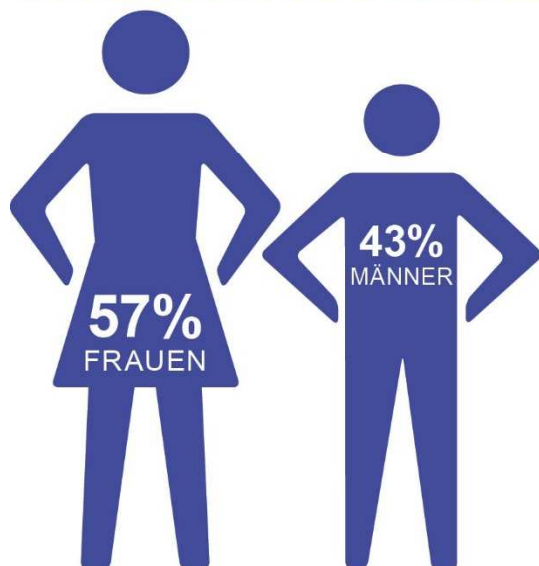
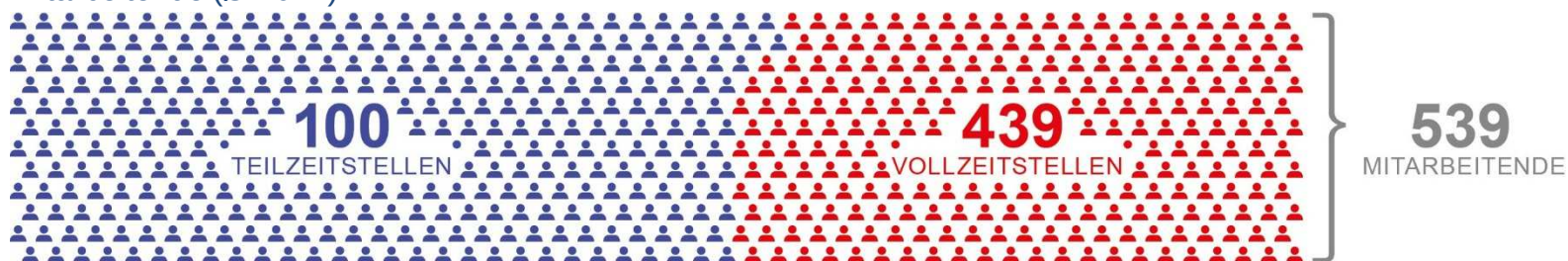


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Das BAG in Zahlen

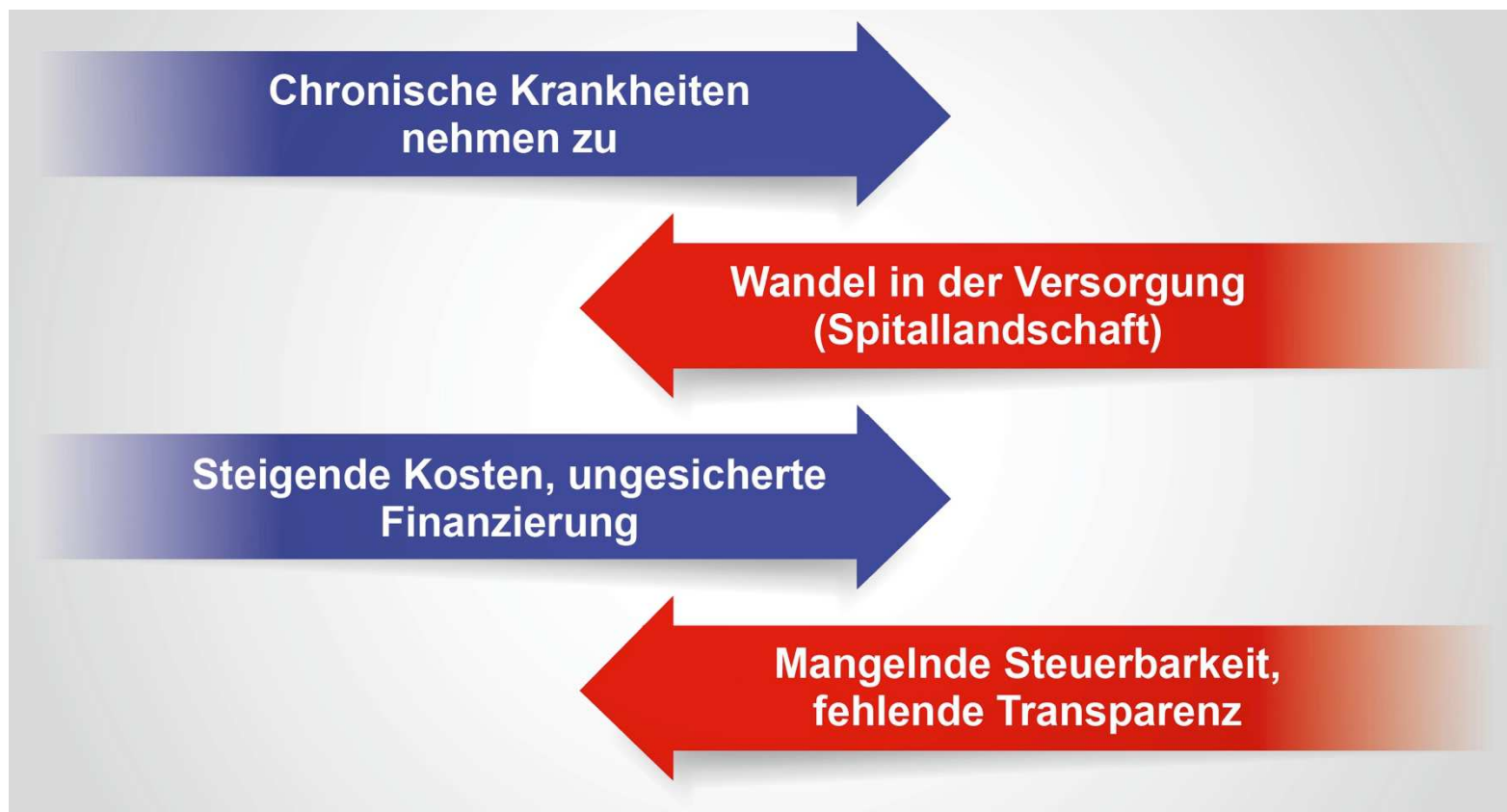
Mitarbeitende (Ø 2014)



Bundesamt für Gesundheit BAG
Abteilung Gesundheitsstrategien, Nicolai Lütchg
11.6.2016



Herausforderungen für das Gesundheitssystem

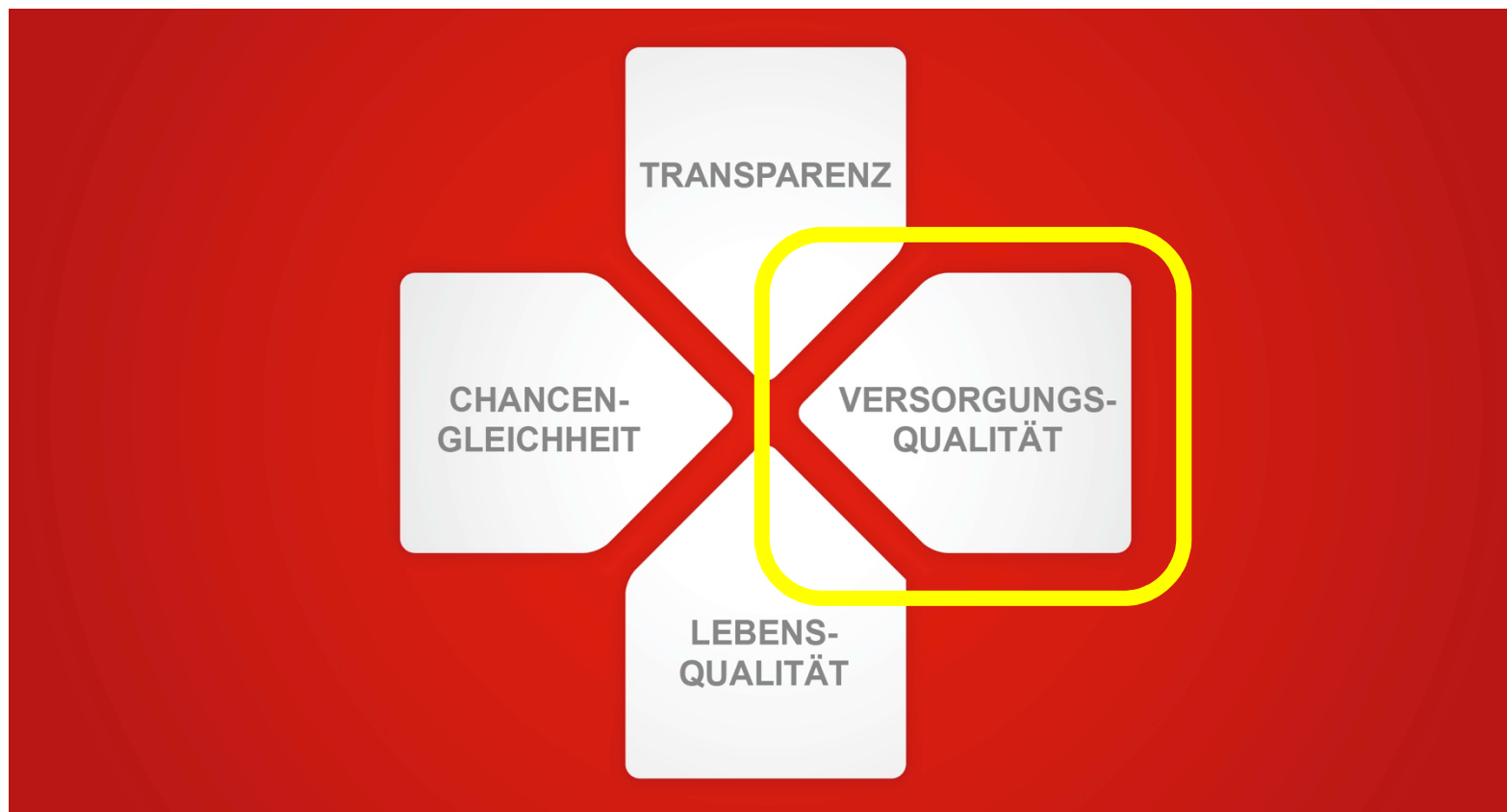




Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Gesundheit2020: Handlungsfelder





Gesundheit2020: Versorgungsqualität



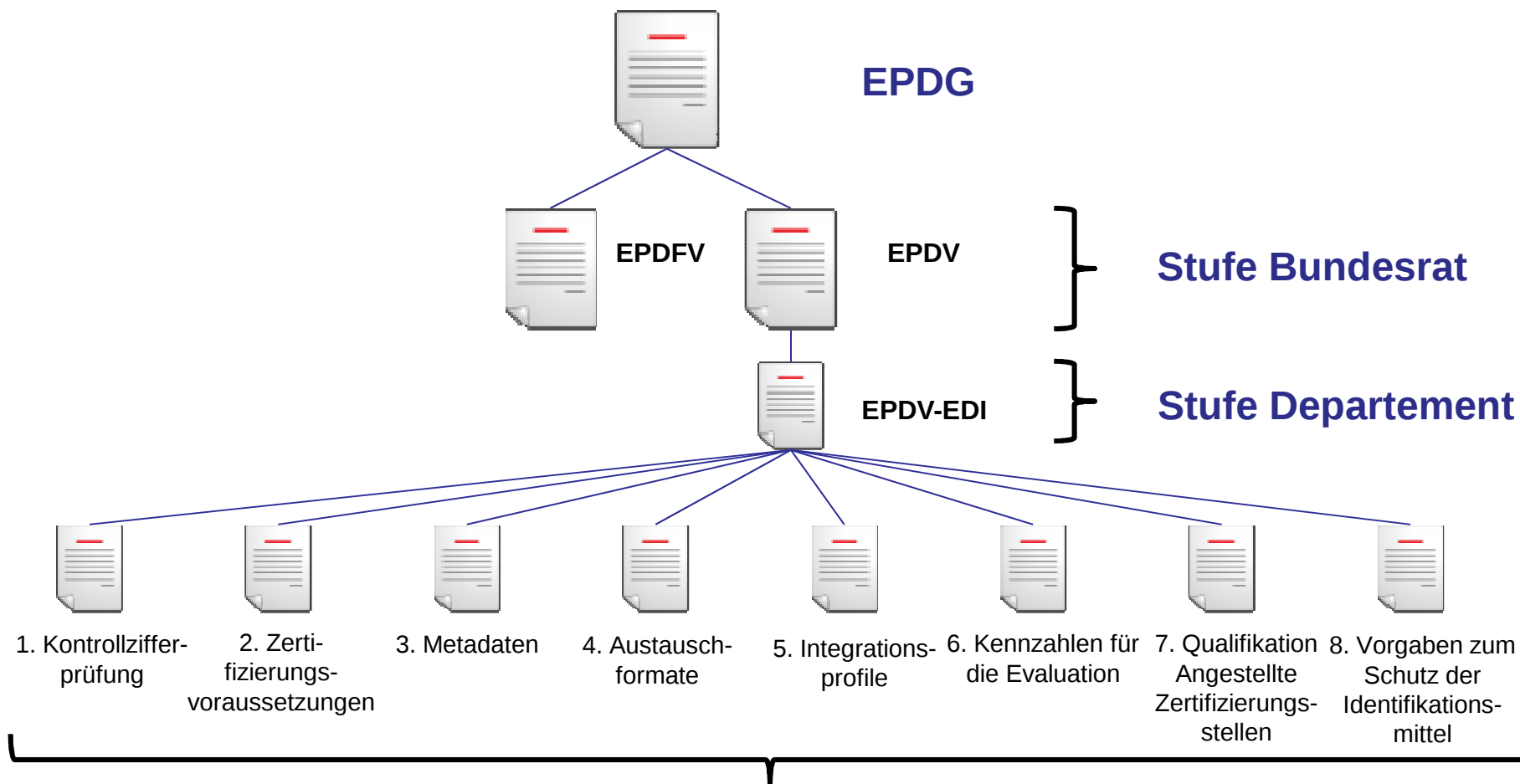


Stand der Dinge – Zeitplan

Dezember 2014	Informationsveranstaltung über Vorgehen und Fragestellungen
Mai 2015	Informationsveranstaltung zu den Kernelementen des Ausführungsrechts
19. Juni 2015	Das EPDG wird von den Räten genehmigt
23. März –	Formelle Anhörung zum VO-Paket nach VIG
29. Juni 2016	
Dezember 2016	Bundesratsbeschluss Inkrafttreten Gesetz und Ausführungsrecht
Q1 2017	geplantes Inkrafttreten des EPDG inkl. Ausführungsrecht



Übersicht über das Ausführungsrecht

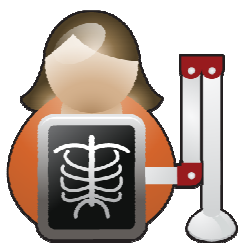




Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Datenschutz und Datensicherheit: mehrdimensional!



Patientin / Patient

Gesundheitsfachpersonen

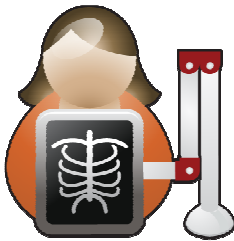
Architektur

«Nutzer»

Bundesamt für Gesundheit BAG
Abteilung Gesundheitsstrategien, Nicolai Lutschg
11.6.2016



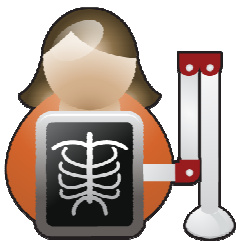
Sicherheit: Patientinnen und Patienten



- Teilnahme freiwillig
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- Umfassende Steuerung der Zugriffsrechte
- Identifikation / Elektronische Identität



Sicherheit: Patientinnen und Patienten



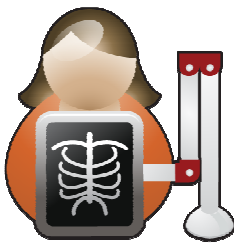
- **Teilnahme freiwillig**
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- Umfassende Steuerung der Zugriffsrechte
- Identifikation / Elektronische Identität

Patientinnen und Patienten durch Nutzen überzeugen

→ Zwang kontraproduktiv



Sicherheit: Patientinnen und Patienten

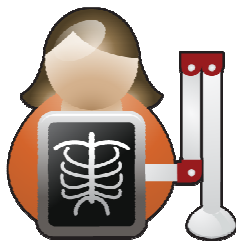


- Teilnahme freiwillig
- **Schriftliche Einwilligung**
- Widerruf jederzeit formlos möglich
- Umfassende Steuerung der Zugriffsrechte
- Identifikation / Elektronische Identität

Umfassende, verständliche Information vor Eröffnung eines EPD
obligatorisch



Sicherheit: Patientinnen und Patienten

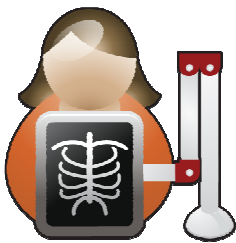


- Teilnahme freiwillig
- Schriftliche Einwilligung
- **Widerruf jederzeit formlos möglich**
- Umfassende Steuerung der Zugriffsrechte
- Identifikation / Elektronische Identität

- Zugriffsrechte der GFP werden entzogen
- Löschung der Dokumente / Links zu den Dokumenten
- «Löschung» der Patientenidentifikationsnr. bei der ZAS
→ Wiederherstellung des Zustands vor der Einwilligung



Sicherheit: Patientinnen und Patienten

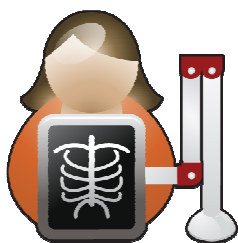


- Teilnahme freiwillig
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- **Umfassende Steuerung der Zugriffsrechte**
- Identifikation / Elektronische Identität

- Patient kann Grundeinstellung der Zugriffsrechte jederzeit ändern
- lesbare Zugriffsprotokolle für Patienten
- Zugriffsrechte können nur vom Patienten oder durch von ihm autorisierte Personen geändert werden
- Blacklist (Ausschlussliste)
- Benachrichtigungen nach Notfallzugriffen



Sicherheit: Patientinnen und Patienten



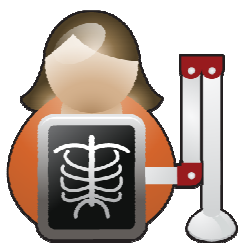
- Teilnahme freiwillig
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- **Umfassende Steuerung der Zugriffsrechte**
- Identifikation / Elektronische Identität

4 Zugriffsstufen:

- nützliche Dokumente (z.B. Allergiepass)
- medizinische Dokumente (z.B. Austrittsbericht)
- sensible Dokumente (z.B. HIV-Befund)
- geheime Dokumente (z.B. Psychiatriebefund)



Sicherheit: Patientinnen und Patienten

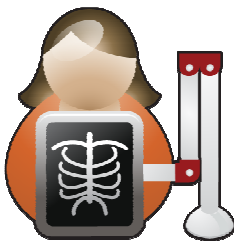


- Teilnahme freiwillig
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- Umfassende Steuerung der Zugriffsrechte
- **Identifikation / Elektronische Identität**

- Keine Verwendung der AHVN13 (Patientenidentifikationsnummer als neuer eindeutiger Identifikator)



Sicherheit: Patientinnen und Patienten



- Teilnahme freiwillig
- Schriftliche Einwilligung
- Widerruf jederzeit formlos möglich
- Umfassende Steuerung der Zugriffsrechte
- **Identifikation / Elektronische Identität**

- Anforderungen an die eID definiert der Bundesrat:
 - o **Das Verfahren:** *Mindestens* Sicherheitsstufe 3 «erhebliche Sicherheit» gem. ISO/IEC 29115
 - o **Das Identifikationsmittel:** muss das Schutzprofil (Anhang 8, EPDV-EDI) erfüllen
- Herausgeber der eID muss zertifiziert sein (Ausgabeprozess, generelle Datensicherheit, etc.)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Sicherheit: Gesundheitsfachpersonen



- Zugriffsrechte müssen bestehen
- Notfallzugriff löst Notifikation aus
- Protokollierung der Zugriffe
- Elektronische Identität



Sicherheit: Gesundheitsfachpersonen



- **Zugriffsrechte müssen bestehen**
- Notfallzugriff löst Notifikation aus
- Protokollierung der Zugriffe
- Elektronische Identität

- Patient erteilt individuelle Zugriffsrechte
- Bei Zugriffsrechten für Gruppen von Gesundheitsfachpersonen: Zusammensetzung muss ersichtlich sein



Sicherheit: Gesundheitsfachpersonen



- Zugriffsrechte müssen bestehen
- **Notfallzugriff löst Notifikation aus**
- Protokollierung der Zugriffe
- Elektronische Identität

- Wenn eine Gesundheitsfachperson mittels Notfallzugriff auf das EPD einer Patientin oder eines Patienten zugreift, wird diese oder dieser schriftlich oder elektronische Benachrichtigt



Sicherheit: Gesundheitsfachpersonen



- Zugriffsrechte müssen bestehen
- Notfallzugriff löst Notifikation aus
- **Protokollierung der Zugriffe**
- Elektronische Identität

- Jeder Zugriff auf das EPD einer Patientin oder eines Patienten wird im Protokoll («Audit Log») verzeichnet
- Auch erfolglose Zugriffe werden protokolliert



Sicherheit: Gesundheitsfachpersonen



- Zugriffsrechte müssen bestehen
- Notfallzugriff löst Notifikation aus
- Protokollierung der Zugriffe
- **Elektronische Identität**

- Anforderungen an die eID definiert der Bundesrat:
 - o **Das Verfahren:** *Mindestens* Sicherheitsstufe 3 «erhebliche Sicherheit» gem. ISO/IEC 29115
 - o **Das Identifikationsmittel:** muss das Schutzprofil (Anhang 8, EPDV-EDI) erfüllen
- Herausgeber der eID muss zertifiziert sein (Ausgabeprozess, generelle Datensicherheit, etc.)

Bundesamt für Gesundheit BAG

Abteilung Gesundheitsstrategien, Nicolai Lütischg

11.6.2016



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

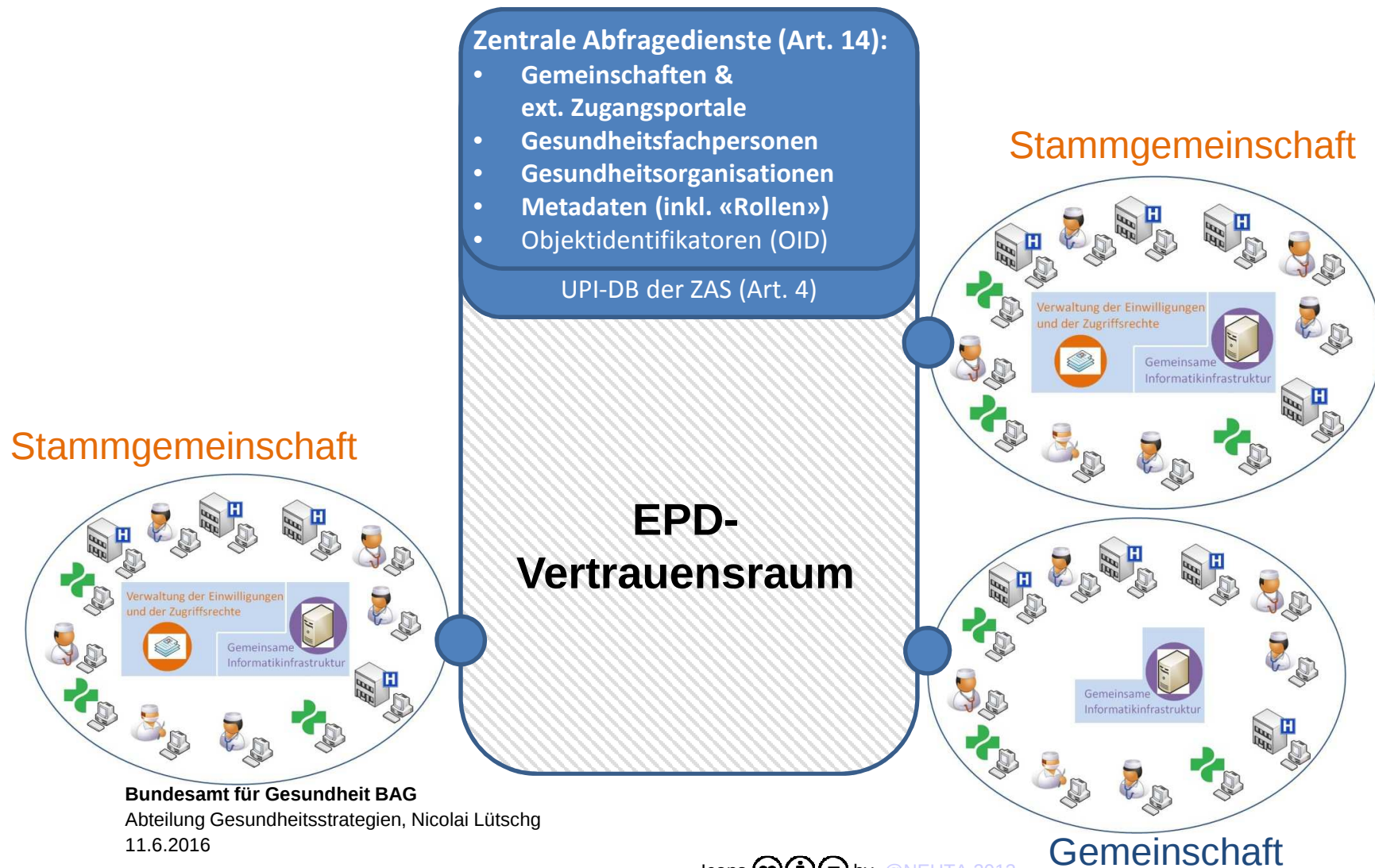
Sicherheit: Architektur

- Dezentrale Architektur
- Zertifizierung von Gemeinschaften und Stammgemeinschaften





Sicherheit: dezentrale Architektur





Sicherheit: dezentrale Architektur

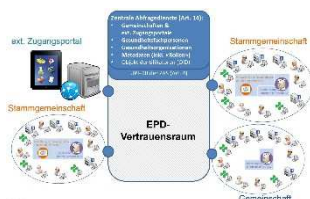
- **Dezentrale Architektur**
- Zertifizierung von Gemeinschaften und Stammgemeinschaften



- kein nationaler zentraler Patientenindex
– *föderierte Master Patient Index-Infrastruktur*
- kein nationaler zentraler Dokumentenspeicher
– *Dokumente bleiben, wenn immer möglich, beim Ersteller*
- föderierter Zusammenschluss verteilter EPD-Komponenten auf Basis von internationalen Standards → IHE, OASIS, etc.



Sicherheit: Zertifizierung

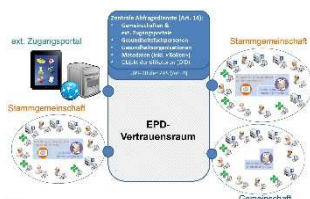


- Dezentrale Architektur
- **Zertifizierung von Gemeinschaften und Stammgemeinschaften**

- Interoperabilität
 - Anwendung von Normen, Standards und Integrationsprofilen
 - Basiert grösstenteils auf den Vorarbeiten von eHealth Suisse
 - Verwendung internationaler Standards



Sicherheit: Zertifizierung



- Dezentrale Architektur
- **Zertifizierung von Gemeinschaften und Stammgemeinschaften**

- Datenschutz / Datensicherheit
 - Vorgaben in der EPDV / TOZ:
 - o Nutzung bestehender Standards (z.B. ISO/IEC 27001)
 - o sicherer Anschluss der Primärsysteme
 - o Meldepflicht für sicherheitsrelevante Ereignisse
 - o Verfügbarkeit der Systeme
 - o Verschlüsselung, etc.

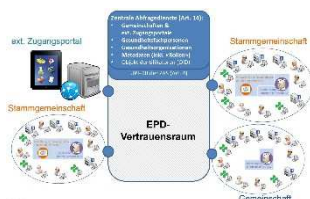
Bundesamt für Gesundheit BAG

Abteilung Gesundheitsstrategien, Nicolai Lütischg

11.6.2016



Sicherheit: Zertifizierung



- Dezentrale Architektur
- **Zertifizierung von Gemeinschaften und Stammgemeinschaften**

- Organisatorische Voraussetzungen
 - Prozesse zur Verwaltung von:
 - o Patientinnen und Patienten (z.B. korrekte Information)
 - o Gesundheitsfachpersonen (Ein-, Austritt, etc.)
 - o Institutionen des Gesundheitswesens



Fazit

- Datenschutz und Datensicherheit kritisch für Akzeptanz des EPD
- Abwägung zwischen Wirtschaftlichkeit und Sicherheit (Zertifizierung von Gemeinschaften und Stammgemeinschaften) **zentral**
→ Gründliche Risikoanalyse als Basis für Anforderungen an Gemeinschaften
- Enge Zusammenarbeit mit Stakeholdern (Datenschützer, Industrie, Zivilgesellschaft)





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Herzlichen Dank

Nicolai Lütschg, Projektleiter EPDG
eHealth@bag.admin.ch