Bei Patienten und Mitarbeitenden Vertrauen für sicheren Umgang mit KIS und EPD schaffen

Information Security in Health Conference, 14. Juni 2016

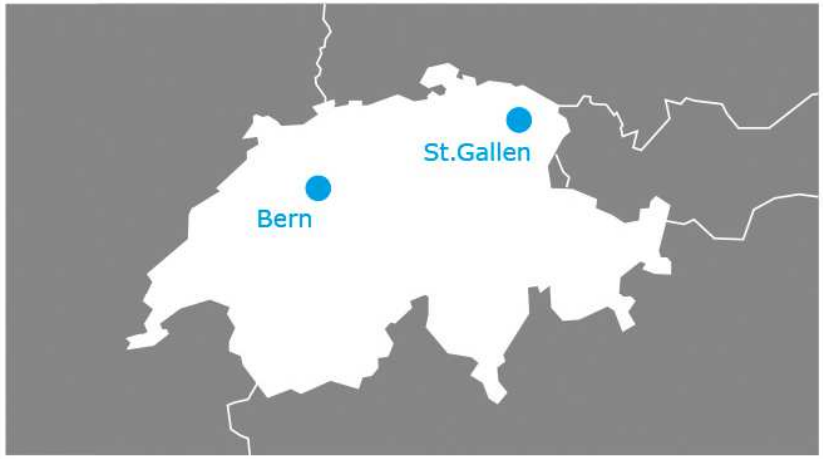
Christoph Knöpfel / Christian Dolf

Einleitung

Die digitale Transformation ist verheissungsvoll…

… vielleicht stecken dahinter verborgene Gefahren?!

Ihr unabhängiger Partner



Aktiengesellschaft seit 1998 (zu 100% bei Mitarbeitenden)
Ca. 20 Beratende / Projektleitende
Über 250 Jahre Projekterfahrung
Hohes Ausbildungsniveau
Backoffice inkl. Auszubildende
Interne Branchenteams mit Innovationsaufträgen
Zahlreiche Partnerschaften & Mitgliedschaften

CSP AG Competence Solutions Projects www.csp-ag.ch

Erfahrungen aus hunderten Projekten

Strategie
Strategiecontrolling
IT Governance Sourcing Business Analyse
E-Government
Reviews Kooperationen
Veränderungsmanagement Prozess-Engineering
Audits Organisationsentwicklung Projektportfolio-Management
Reorganisationen
Supply Chain Management
Innovation
Service-Management
Moderation Coaching
Knowledge-Management
GEVER CMS KIS
Records-Management
Projektcontrolling
Studien / Konzeptionen Enterprise Content Management
Interim-Management Requirements-Engineering SLA-Management
Expertisen Schulungen Benchmarking Schulinformatik Submissionen
Evaluationen IT-Vertragsmanagement IT-Einführungen
Informationssicherheit Projektmanagement ERP
Kontinuitätsmanagement Ausschreibungen
Qualitätsmanagement Risikomanagement Testmanagement
Business Continuity Management
Workflow-Management

Agenda

1. Sicherheit und Vertrauen in der eigenen Organisation
2. Sicherheit und Vertrauen in der Vernetzung
3. Fazit und Diskussion

Ohne Behandlungsdaten keine Patientenbehandlung

Informationen über einen Patienten ist wie das Seil einer Seilschaft für die Bergbesteigung.

Sicherheit und Vertrauen in der eigenen Institution

Nur sollten diejenigen Personen einem bekannt und vertraut sein, mit denen man eine Seilschaft eingeht.

Behandlungsdaten als Arbeitswerkzeug

Ohne Informationen zu einem Patienten, fehlen Informationen

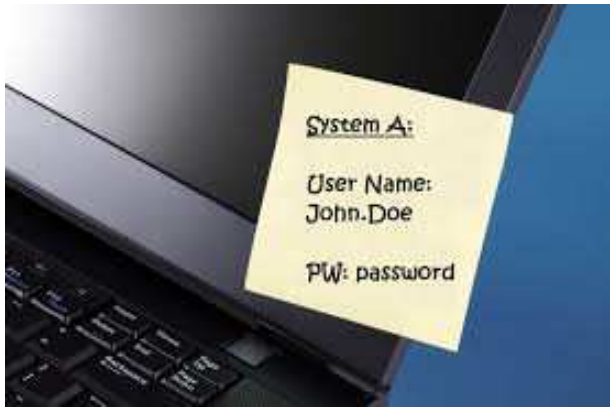
- zur Vorgeschichte,
- zu den schon bekannten medizinischen Rahmenbedingungen (Diagnosen, Therapien, Risiken, …)
- und seinem sozialen Umfeld.

Sicherheit und Vertrauen in der eigenen Institution

Beispiel: Behandlung geriatrische frührehabilitative Komplexbehandlung

Um schnell festzustellen, dass mit der korrekten Behandlung eine Entlassung in das angestammte Umfeld möglich ist, müssen sehr viele Informationen mit einander abgeglichen werden.

Um diese Informationen beschaffen zu können, werden IT-Sicherheitsbestimmungen von Anwendern als sehr störend empfunden.



Eigene Mitarbeiter als Patienten

Sicherheit und Vertrauen in der eigenen Institution

Sobald ein Mitarbeiter einer Gesundheitseinrichtung selbst zu einem Patienten wird, ändert sich die Sensitivität für die Informationsverteilung.

Trotz VIP Kennzeichnung müssen die Behandlungsinformation häufig offen gelegt werden;

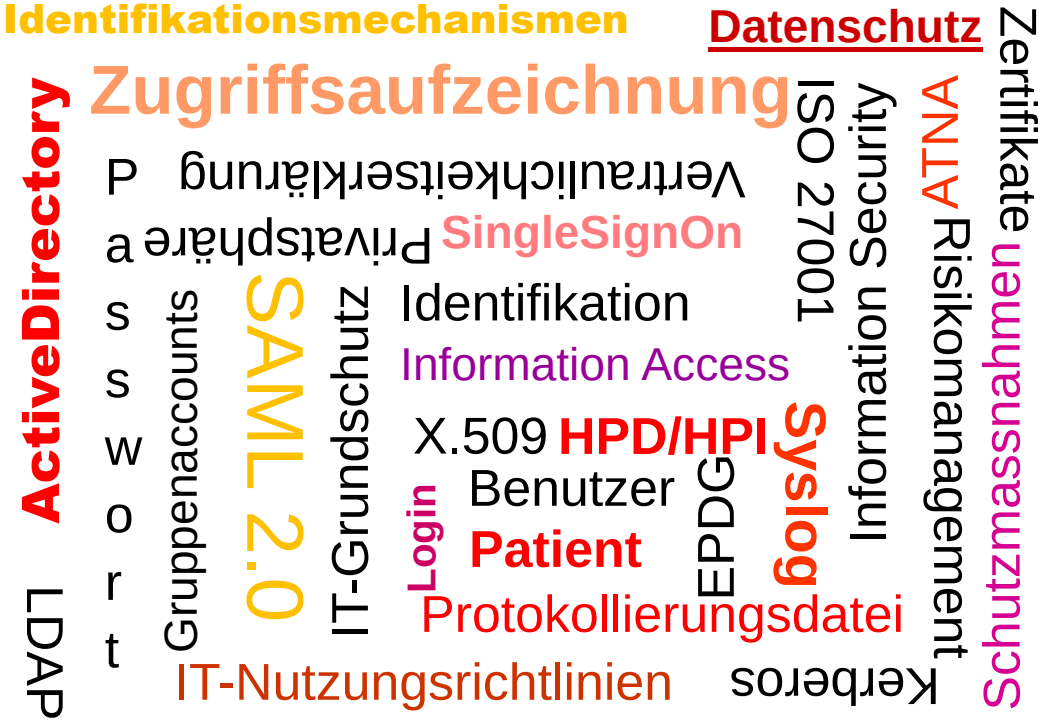
- da nicht alle IT-Systeme die VIP Kennzeichnung unterstützen,
- sehr viele Personen den Zugriff für Behandlung (direkt und indirekt) benötigen
- und die Gefahr besteht, dass wichtige Informationen nicht beachtet werden.

Herausforderungen für die Massnahmen innerhalb der eigenen Institution

Alle vorgeschlagenen Massnahmen dienen der Schaffung von mehr Transparenz im Umgang mit Informationssicherheit innerhalb einer Organisation.

Dabei kann auf etablierte Technologien und bekannte Standards gesetzt werden.

Sicherheit und Vertrauen in der eigenen Institution



Beispiele von Massnahmen für die verstärkte Wahrnehmung der Informationssicherheit in der Organisation

Sicherheit und Vertrauen in der eigenen Institution

Anhand von 3 Beispielen wollen wir mögliche Massnahmen aufzeigen:

- Regelmässige IT-Sicherheitssprechstunden innerhalb der Organisation durchführen
- Vorgaben aus dem EPDG auch innerhalb der Organisation umsetzen
  - Zugriffsaufzeichnungen zentralisieren und die entsprechenden Auswertungen den Betroffenen zur Verfügung stellen
  - Einverständniserklärung zur elektronischen Verarbeitung von Behandlungsdaten innerhalb der Organisation nutzbar machen

Transparenz auch im Umgang mit IT-Sicherheitstechnologien

IT-Sicherheitssprechstunden

IT-Sicherheitssprechstunden ermöglichen innerhalb einer Organisation das Thema Informationssicherheit direkt bei den Anwendern vor Ort transparenter zu machen.

Vorteile:

Sicherheit und Vertrauen in der eigenen Institution

- Es lässt sich in bestehende interne Weiterbildungsprogramme integrieren
- Anhand von aktuellen Beispielen aus den Medien oder innerhalb der Organisation kann das Bewusstsein für Informationssicherheit gestärkt werden
- Es bietet den Anwendern die Möglichkeit ihre Ängste und Sorgen platzieren zu können

Zentrale Aufzeichnung der Zugriffsprotokolle

Mit der Einführung des EPDG wird für das Patientendossier die Zusammenführung aller Zugriffsprotokolle in einen Service verlangt. Die gleiche Technologie kann für die Zugriffe innerhalb einer Organisation verwendet werden.

Dadurch ergeben sich folgende Vorteile:

Sicherheit und Vertrauen in der eigenen Institution

- Die Sensibilität der Anwender wird gesteigert, wenn ihnen ihre Zugriffe transparent gemacht werden
- Der Aufwand für das EPDG kann auch für die Informationssicherheit innerhalb einer Organisation genutzt werden
- Bei rechtlichen Abklärungen kann der Aufwand für die Informationsbeschaffung reduziert werden
- Es wird eine bestehende Technologie eingesetzt, die international durch die IHE (www.ihe.net) seit ca. 2004 in Tests überprüft werden.

IHE Integrating the Healthcare Enterprise

Einverständniserklärung zur elektronischen Verarbeitung von Behandlungsinformationen

Sicherheit und Vertrauen in der eigenen Institution

Mit der Einführung des EPDG wird neu erwartet, dass der Patienten seine Einverständniserklärung zur elektronischen Verarbeitung der Behandlungsinformationen bei Bedarf verändern kann. Dazu werden wie bei den Zugriffsprotokollen bestehende Standards vorgeschlagen. Wenn dies auch innerhalb der Organisation umgesetzt wird, kann insbesondere auch der eigene Mitarbeiterschutz verbessert werden.

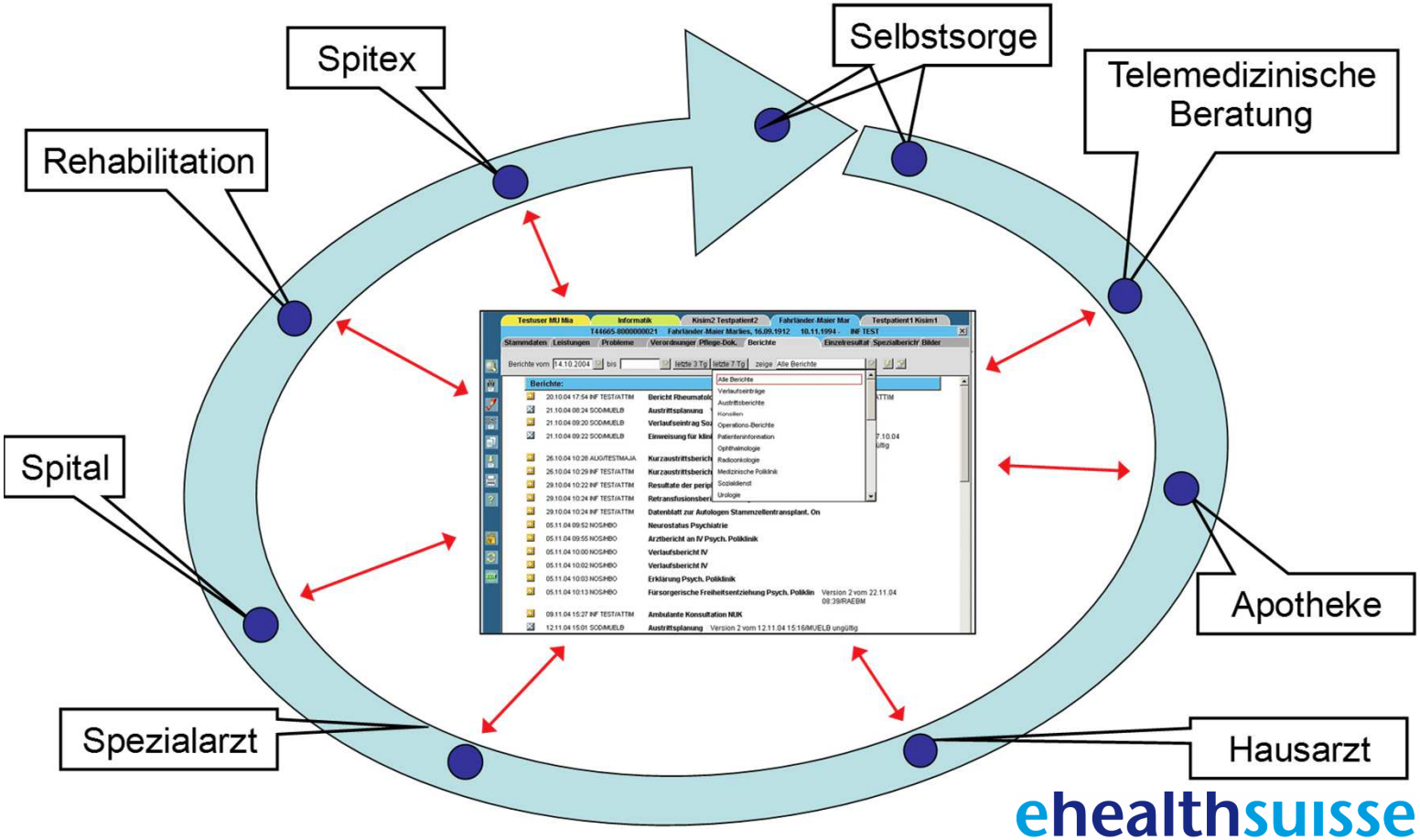
Umfragen zeigen, dass die betroffenen Personen das am liebsten mit ihrem Vertrauensarzt (in der Regel Hausarzt) klären. Für die Mitarbeiter könnte dies über den personalärztlichen Dienst angeboten werden.

Dadurch ergeben sich folgende Vorteile:

- Die Einwilligung kann auf bestehende Kriterien (Organisationseinheiten, Behandlungspfade, besonders sensitive Informationen, …) festgelegt werden und ist nicht nur eine globale Einwilligung
- Der Patient hat die Möglichkeit je nach Umstand selbst die Einwilligung zu lockern oder zu verschärfen

… und in der vernetzten Gesundheitsversorgung?

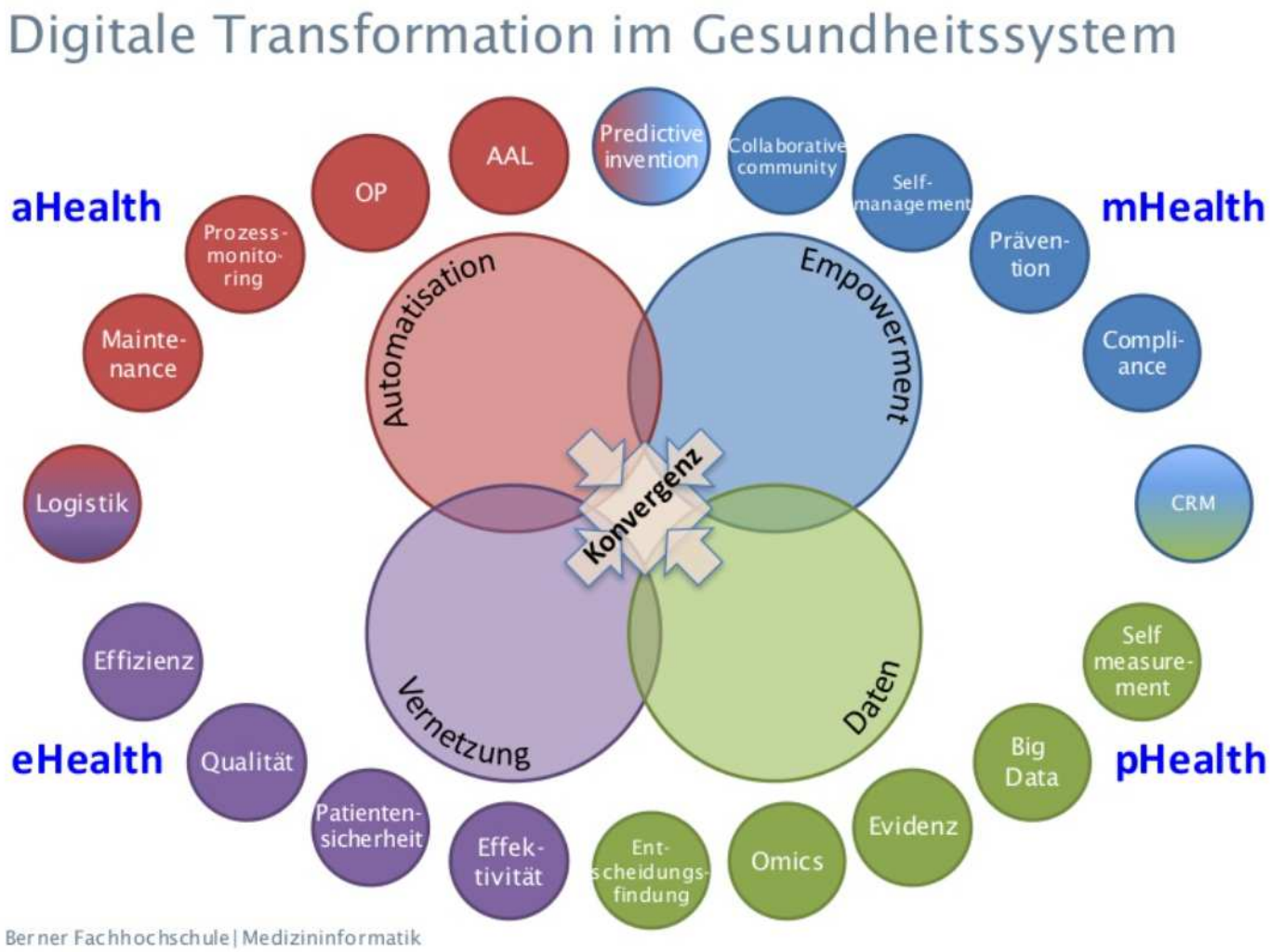
Sicherheit und Vertrauen in der Vernetzung



ehealthsuisse
Koordinationsorgan Bund-Kantone

… und in der vernetzten Gesundheitswelt?

Sicherheit und Vertrauen in der Vernetzung



Sicherheit und Vertrauen in der Vernetzung

Sicherheit bringt Nutzen, ist aber auch aufwändig!

Im Zentrum stehen die Schlüsselfaktoren…

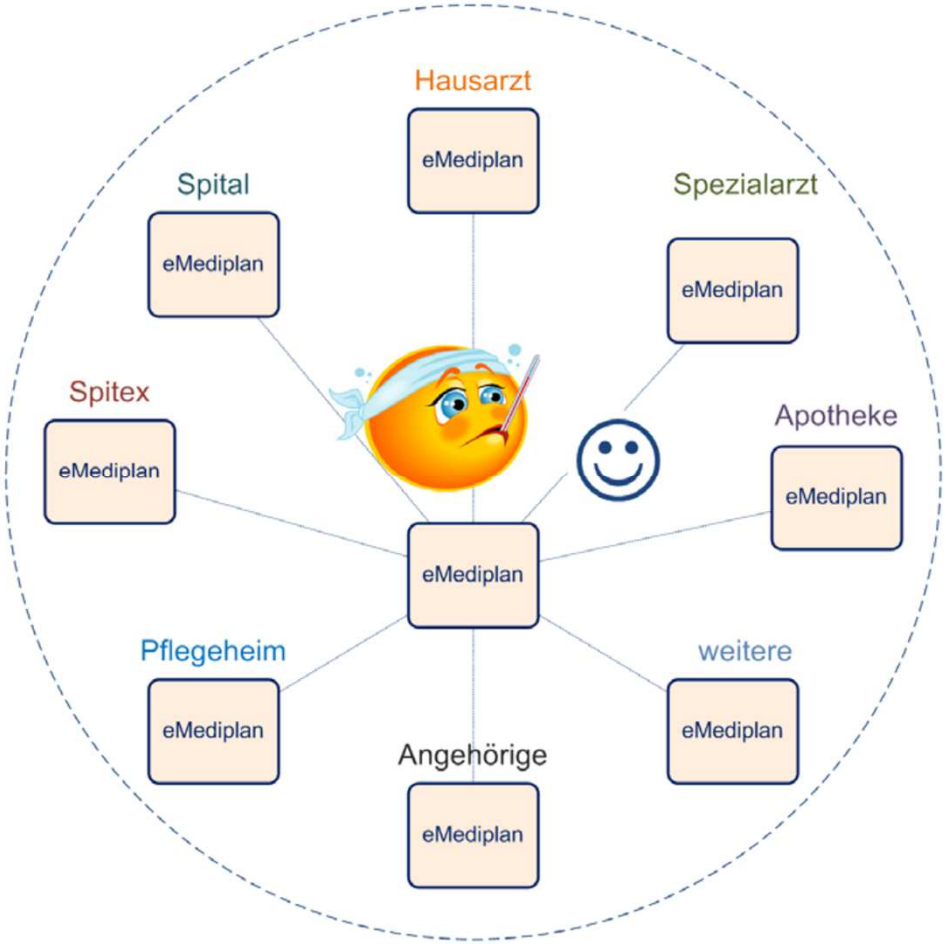
Sicherheit und Vertrauen in der Vernetzung

Nutzen und…

… Vertrauen

Beispiel: eMediplan im Verbund

Sicherheit und Vertrauen in der Vernetzung



- ein Patient
- viele Akteure
- ein vollständiger, aktueller Medikamentenplan
- zum Nutzen aller Beteiligter, nicht zuletzt des Patienten.

Nutzen: Darum eMediplan

Sicherheit und Vertrauen in der Vernetzung

- Die **Arzneimitteltherapiesicherheit** wird verbessert.
- Die unbefriedigende Situation an den **Schnittstellen** zwischen den Leistungserbringern wird angegangen (**Integrierte Versorgung**).
- Die **Erwartungen** der Patienten und deren Angehörigen werden erfüllt.
- Die **heutigen technologischen Möglichkeiten** werden zur Optimierung des Medikationsprozesses genutzt…

Gemeinsam erarbeitete und breit akzeptierte fachliche Anforderungen an eMediplan

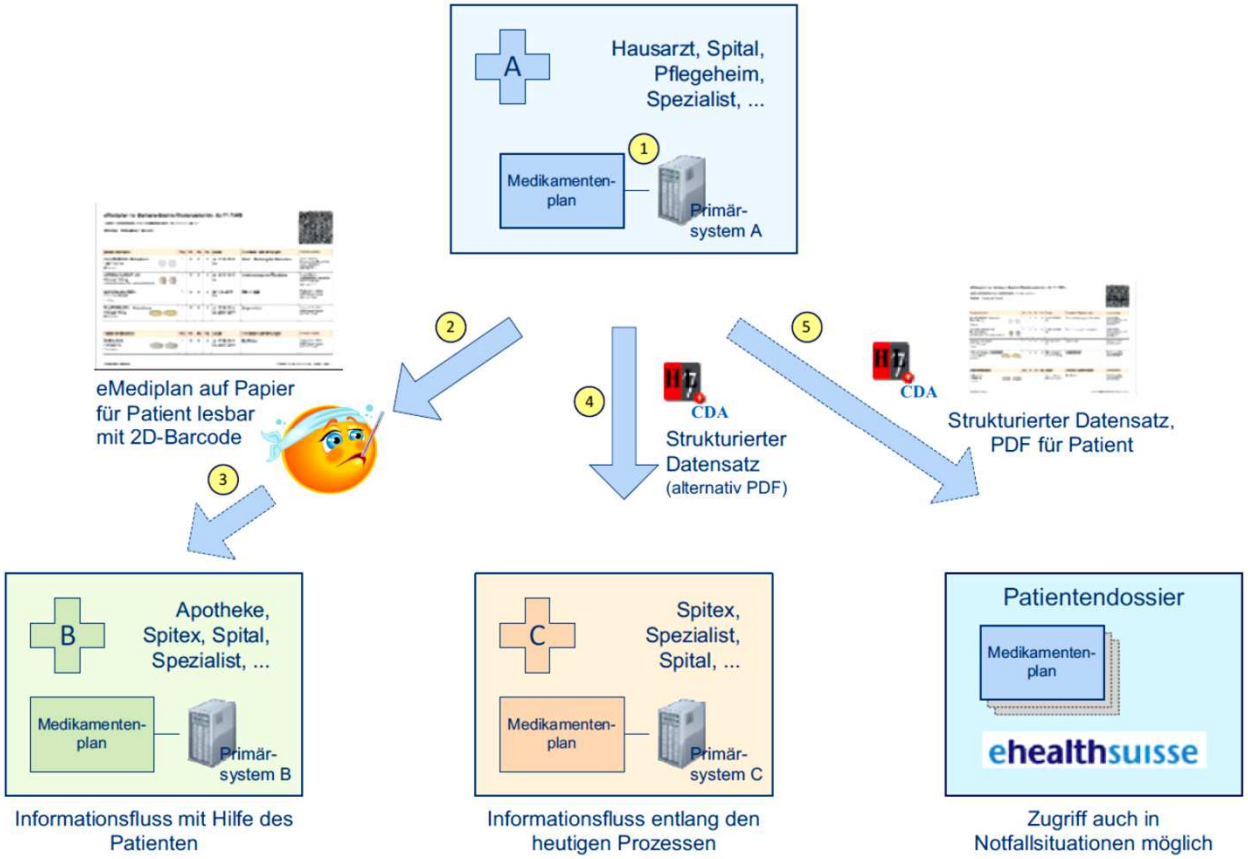
Sicherheit und Vertrauen in der Vernetzung

- **Patienten** müssen ihre aktuelle, vollständige Medikation kennen.
- Die Medikation muss **jeder Gesundheitsfachperson**, die verordnet, substituiert oder Medikamente für den Patienten bereitstellt, aktuell und vollständig bekannt sein.
- Die vollständige Medikation muss **im eigenen Informationssystem** der Leistungserbringer dokumentiert sein.
- Die **Kommunikation** zwischen den Leistungserbringern muss verbessert werden. Dabei müssen das Patientengeheimnis und der Datenschutz respektiert werden.
- Die angestrebte Lösung muss mit dem elektronischen Patientendossier und den Empfehlungen von **eHealth Suisse kompatibel** sein.
- Die angestrebte Lösung muss **schrittweise eingeführt** werden können und muss **bezahlbar** sein.

Umsetzung in verdaubaren Etappen

bezüglich Funktionalität, Beteiligte, Termine, Quick-Wins, Finanzen…

Sicherheit und Vertrauen in der Vernetzung



→ Gemeinsam (Sicherheit) lernen und Vertrauen bilden!

Massnahmen und kritische Erfolgsfaktoren

Sicherheit und Vertrauen in der Vernetzung

Rechtliche Grundlage

Sichere Infra-struktur/Zugang

Transport/ Verpackung

Passende Use Cases

Information Kommunikation

Orchestrieren über Kooperation!

Vertrauen für Informationssicherheit & Datenschutz

Inhalte/ Semantik

Begleitung/ Befähigung

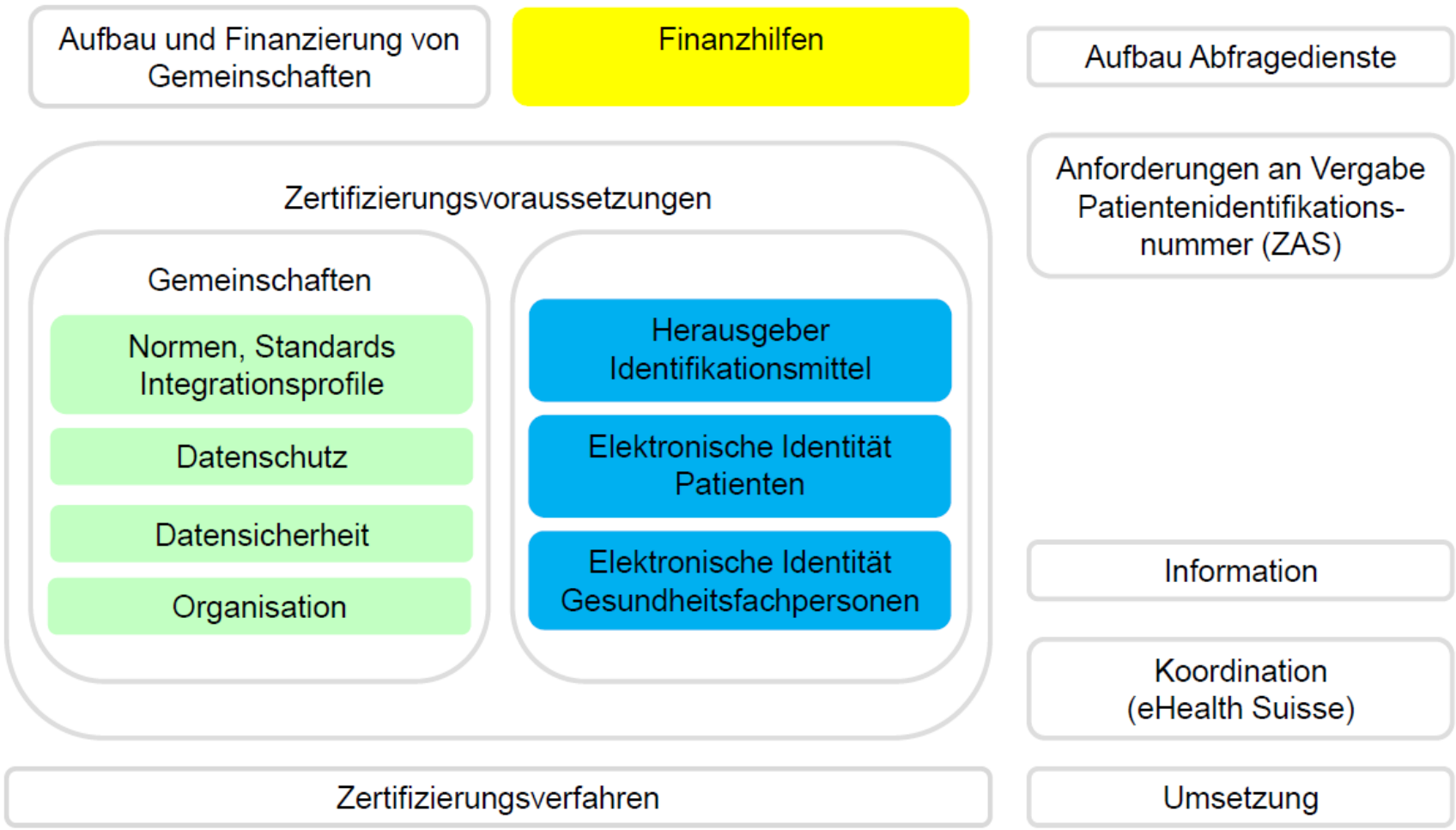
(Aus- & Weiter) Bildung

Finanzierungs-modelle

«Spielregeln» Policies

… im Zusammenhang mit dem EPDG

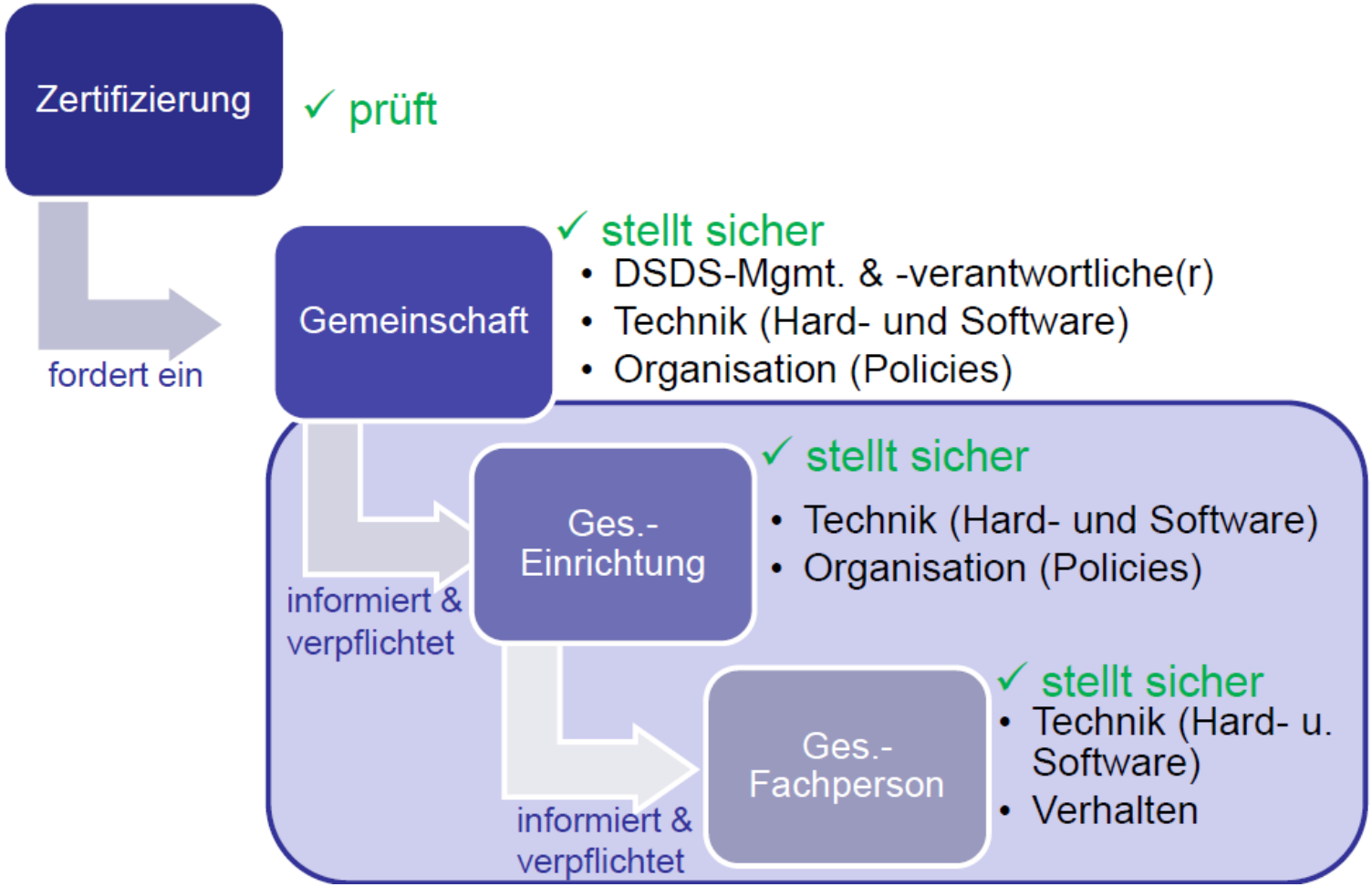
Sicherheit und Vertrauen in der Vernetzung



EPDG-Regelungen

Sicherheit und Vertrauen in der Vernetzung

Datenschutz und Datensicherheit (Art. 11 EPDV) - Übersicht



Grundeinstellung der Zugriffsrechte

Sicherheit und Vertrauen in der Vernetzung

Zugriffsreche von Gesundheitsfachpersonen (Art. 1-3 EPDV)

		Vertraulichkeitsstufen der Dokumente			
		Nützliche Daten	Medizinische Daten	Sensible Daten	Geheime Daten
Zugriffsrechte	Eingeschränkt	✓	×	×	×
	Normal	✓	✓	×	×
	Erweitert	✓	✓	✓	×
	Notfall	✓	✓	×	×

✓ = berechtigte Gesundheitsfachperson kann auf die Dokumente zugreifen

× = Gesundheitsfachperson kann nicht auf die Dokumente zugreifen

Blau = Kann durch die Patientin oder den Patienten jederzeit angepasst werden

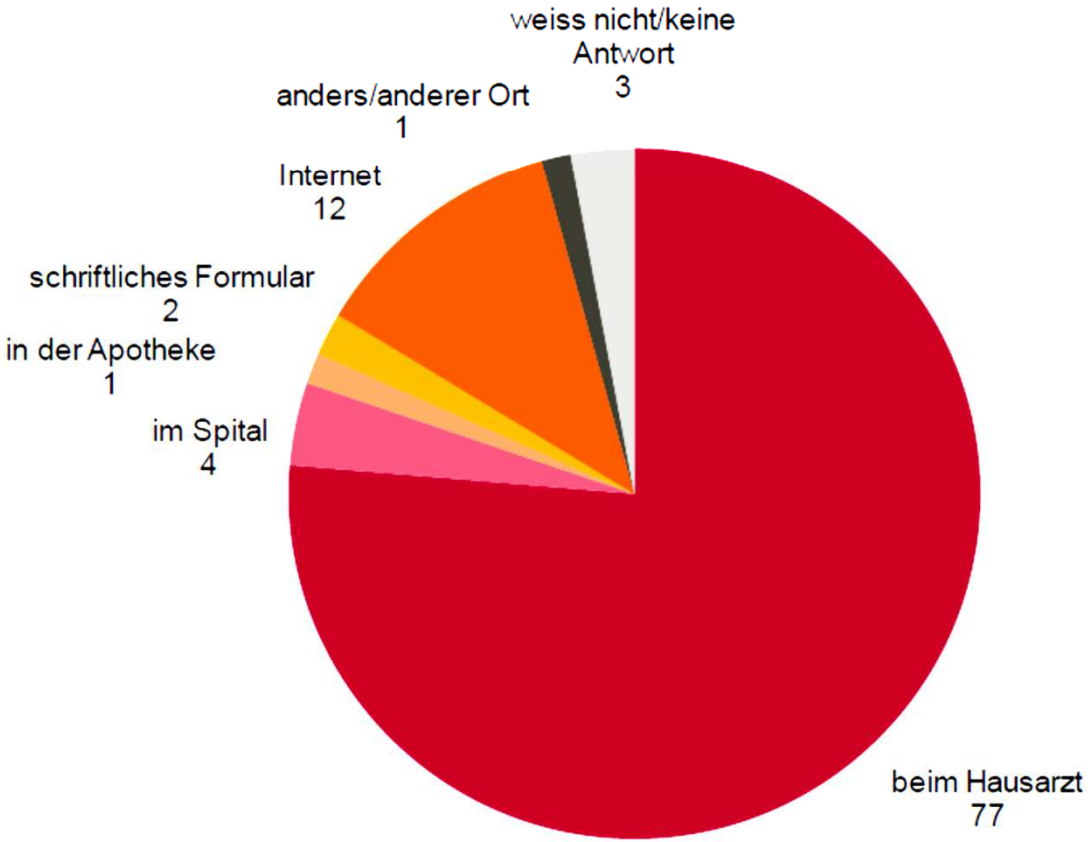
⚠ **Formulierung des Art. 2 Abs. 2 EPDV:**
Nimmt die Patientin oder der Patient keine Zuweisung vor, so gilt das Zugriffsrecht «normal».
–> Gesundheitsfachpersonen können nur auf Daten von Patientinnen oder Patienten zugreifen, soweit diese ihnen entsprechende Zugriffsrechte erteilt haben (vgl. Art. 9, Abs. 1 EPDG)

Unterstützung/Begleitung durch Leistungserbringer

Sicherheit und Vertrauen in der Vernetzung

"Wo würden Sie am liebsten ein elektronisches Patientendossier eröffnen? Beim Hausarzt, im Spital, in der Apotheke, über ein schriftliches Formular oder über Internet?"

in % Stimmberechtigter, die ein elektronisches Patientendossier eröffnen und verwenden würden oder die bei einer Empfehlung durch eine Gesundheitsfachperson bereit wären, eines zu eröffnen



© gfs.bern, Öffentliche Meinung eHealth, Januar 2016 (n = 598)

Konklusion zur Informationssicherheit im vernetzten Gesundheitswesen

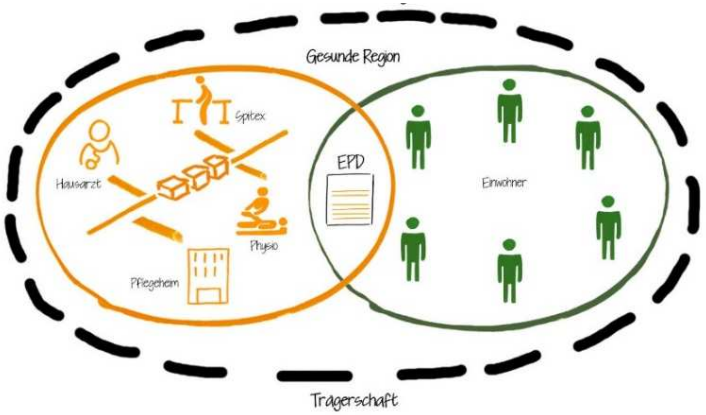
Zahlreiche Massnahmen dienen der Schaffung von mehr Transparenz im Umgang mit Informationssicherheit im vernetzten Gesundheitswesen.

Entscheidend sind:

Sicherheit und Vertrauen in der Vernetzung

- Institutionstyp-übergreifende Kooperation (Spital, Arzt, Pflegeheim, Spitex, Physiotherapie etc.) zur gemeinsame Gestaltung in der «eigenen vernetzten, gesunden Region» (AD),

- der richtige Mix und die Setzung von Prioritäten um Nutzen und Vertrauen zu fördern



- sichere, vertrauenswürdige Übergänge in die anderen Regionen.

Aufruf an Sie…

…unabhängig von der Berufsgruppe empfehlen wir Ihnen folgende Massnahmen:

Fazit und Diskussion

- Erkennen Sie das EPDG und die digitale Transformation als Chance.
- Fördern Sie die gemeinsame Gestaltung und Kooperationen.
- Fällen Sie geschickte Management-Entscheide.
- Unterstützen Sie konkrete Massnahmen in Ihrer Institution zur Sicherheitsförderung.

Diskussion

Herzlichen Dank für Ihre Aufmerksamkeit

Christian Dolf

Direkt +41 71 231 10 81
christian.dolf@csp-ag.ch

Christoph Knöpfel

Direkt +41 71 231 10 77
christoph.knöpfel@csp-ag.ch

CSP AG
Teufener Strasse 5
CH-9000 St.Gallen
Tel +41 71 231 10 60
www.csp-ag.ch