Das EPD im Spannungsfeld von Selbstbestimmung und Datenanalyse

Digitalization by ORBIS and Microsoft

Impulsreferat 14:40 – 15:00

Thomas Kessler, IT-Security Architekt, TEMET AG

28.08.2019

Agenda

- Das EPD: Eine Infrastruktur für das «Spital Schweiz»
- Die informationelle Selbstbestimmung im EPD
- Grenzen, Chancen und Herausforderungen für die Datenanalyse

EPD = Elektronisches Patientendossier

Über den Referenten

Thomas Kessler

Dipl. Physiker ETH
MAS ZFH in Business Administration

IT-Security Architekt, Partner
In der IT-Security tätig seit 1991

Spezialgebiete
Security Architecture and Strategy
Strong Authentiction
Identity Provider (IdP)

Kontakt
Tel: +41 79 508 25 43
E-Mail: thomas.kessler@temet.ch

EPD Referenzprojekte (Auswahl)

- 2019, Stammgemeinschaft: Teilprojektleitung „Zertifizierung“
- 2019, eHS: „Funktionsabnahmen in EPD-Produktivumgebungen“
- 2018, Spital: Unterstützung des EPD-Anbindungsprojekts
- *2018, EPD-Stammgemeinschaft: Mandat als DSDS-Verantwortlicher
- *2017, Spital: Sicherheitsreview EPD-Anbindungskonzept
- *2016, Kanton: AKV für die Informationssicherheit im EPD
- *2015, BAG: Bedrohungs- und Risikoanalyse für das EPD

*: Öffentlich vorgestellte Projekte anlässlich der eHealth Foren 2016/2017/2018/2019

Über die TEMET AG

Die TEMET AG positioniert sich im Markt als unabhängige und auf Security fokussierte Firma, deren Berater fachliche Expertise mit Management und Projektkompetenz verbinden.

Das elektronische Patientendossier (EPD)

Wer macht mit

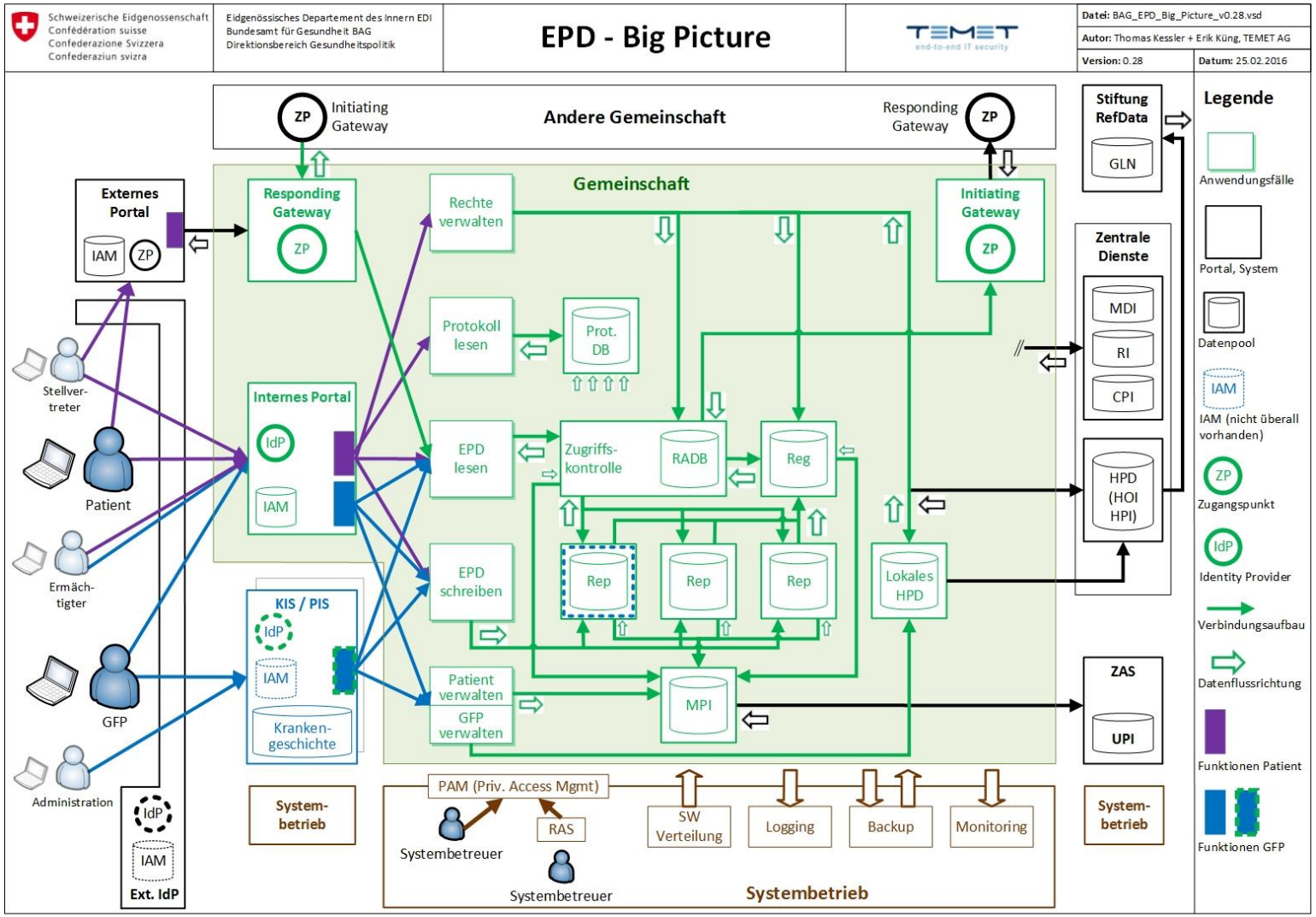
- Ab Sommer 2020 kann jeder Inhaber einer AHVN13 Nummer ein elektronisches Patientendossier (EPD) eröffnen
  - 8 EPD Stammgemeinschaften befinden sich derzeit im Aufbau / im Zertifizierungsprozess
  - Die Stammgemeinschaften sind regional oder nach Berufsgruppe (Apotheker) organisiert
- Ab dann müssen Spitäler, Rehabilitationskliniken und Psychiatrische Kliniken alle behandlungsrelevanten Daten im EPD ablegen
  - Pflegeheime und Geburtshäuser folgen zwei Jahre später
  - Für ambulant tätige Gesundheitsfachpersonen (niedergelassene Ärzte, Apotheker, Spitex,…) ist die Beteiligung am EPD freiwillig
- Die EPD-Gesetzgebung stellt die Interoperabilität zwischen den EPD-Gemeinschaften sicher
  - Wie bei der Telefonie ist eine gemeinschaftsübergreifende Nutzung sichergestellt

Eine Infrastruktur für das «Spital Schweiz»

Bausteine des EPD

- MPI (Master Patient Index)
  - Nationales Verzeichnis aller Patientinnen und Patienten
- HPD (Healthcare Provider Directory)
  - Nationales Verzeichnis aller Gesundheitsfachpersonen und Gesundheitseinrichtungen
- Registry und Policy Server
  - Verzeichnisse aller im EPD abgelegten Dokumente und aller Zugriffsrechte
- Repositories
  - Dokumentenablagen in den Gemeinschaften und den Gesundheitseinrichtungen
- Patientenportal und GFP-Portal
  - Zugriffskanäle für Patienten und Gesundheitsfachpersonen

Das EPD «Big Picture»



Use Cases:

- EPD schreiben
- EPD lesen
- Benutzer verwalten
- Rechte verwalten
- Protokoll lesen

Quelle: "EPD Bedrohungs- und Risikoanalyse" (BAG und Temet, 2015) (URL)

Benutzergruppen

Wer hat Zugriff auf das EPD und wer nicht

- Patientinnen und Patienten können ihr eigenes EPD einsehen und Dokumente in ihrem EPD ablegen
  - Sie können Stellvertreter (z.B. ein Familienmitglied oder eine Gesundheitsfachperson) nominieren, die mit denselben Rechten (aber separater Identität) auf ihr EPD zugreifen
- Gesundheitsfachpersonen und deren Hilfspersonen (z.B. medizinische Sekretariate) können im Behandlungskontext ein EPD einsehen, wenn sie vom Patienten dazu berechtigt worden sind
  - Die Berechtigung kann auch über eine GFP-Gruppe (z.B. Klinik) zugeteilt werden
- Alle anderen Personengruppen (Plattformbetreiber, Klinische Forscher, Krankenversicherer,…) sind vom EPD ausgeschlossen
  - Datenverschlüsselung, Zertifizierungsanforderungen und Zertifizierungsprozess stellen sicher, dass diesbezüglich keine Hintertüren offen sind.

«EPD 1.0»

- Mit dem EPD wird per 2020 eine Basisinfrastruktur gelegt, vergleichbar mit dem nationalen Hochspannungsnetz oder dem Schienennetz
- Der volle Nutzen wird erst in vielen Jahren erzielt werden; in der Analogie fehlen noch elektrische Endgeräte oder Logistikketten
- Die im EPD 1.0 abgelegten Daten sind weitgehend unstrukturiert (PDF), was eine Automatisierung und Analyse sehr schwierig macht
- Der Zugriff auf das EPD 1.0 erfolgt weitgehend manuell über ein Portal (Browser), was die Geschäftsprozessintegration aufwendig macht

⇨ Die kommenden Jahre werden zeigen, ob die Geduld und die Mittel für eine längere Durststrecke ausreichen

Informationelle Selbstbestimmung im EPD

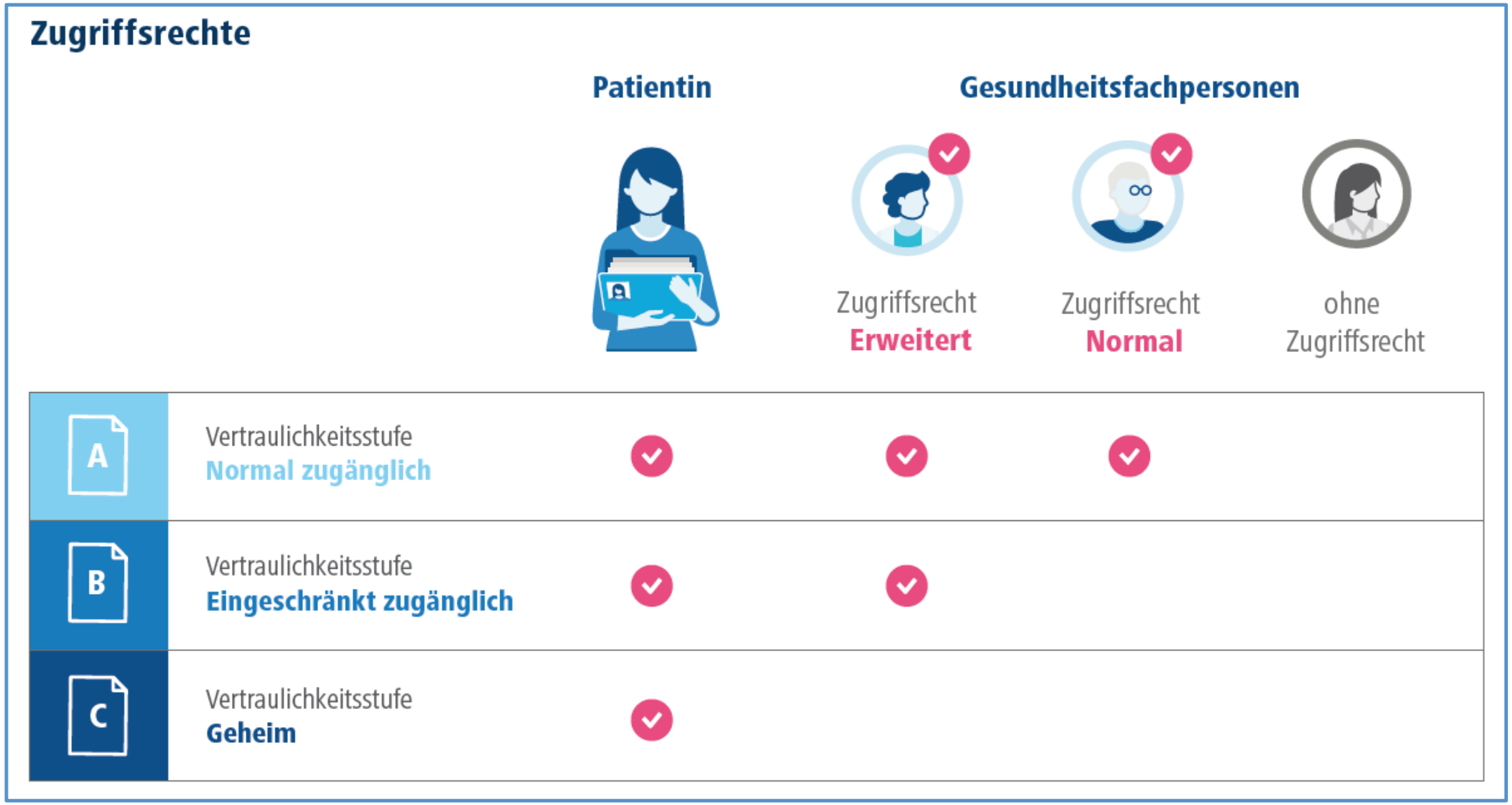
Die im EPD abgelegten Daten gehören den Patientinnen und Patienten:

- Sie bestimmen explizit darüber, wer auf ihr EPD zugreifen kann (siehe Folgefolien für die Details)
- Sie können im EPD Zugriffsprotokoll jederzeit einsehen, wer wann welche Dokumente im EPD abgerufen oder zusätzlich abgelegt hat
- Sie können die im EPD abgelegten Daten jederzeit löschen

Vergabe der EPD-Zugriffsrechte

- Patientinnen und Patienten können…
  - … alle in ihrem EPD abgelegten Dokumente selber und jederzeit einer von drei Vertraulichkeitsstufen zuordnen;
  - … einer Gesundheitsfachperson (GFP) ein normales oder erweitertes Zugriffsrecht erteilen oder diese ganz vom Zugriff auf ihr EPD ausschliessen;
  - … einer Gruppe von GFP ein (immer befristetes) Zugriffsrecht erteilen;
  - … die Verwaltung ihres EPD stellvertretend einer Vertrauensperson übergeben. Dies kann eine Person aus dem privaten Umfeld sein oder eine GFP (z.B. Hausarzt, Spitex);
  - … eine Gesundheitsfachperson ermächtigen, dass sie ihr eigenes Zugriffsrecht auf weitere GFP oder Gruppen von GFP überträgt;
  - … sich darüber informieren lassen, wenn neue GFP einer zugriffsberechtigten Gruppe von GFP beitreten;
  - … die Grundeinstellungen jederzeit ändern.

Zugriffsrechte im EPD



Quelle: "EPD Informationsbroschüre für die Bevölkerung" (eHealth Suisse, 2018)

Die Erteilung von Zugriffsrechten erfolgt unter Berücksichtigung der Datenklassifizierung jedes einzelnen Dokuments

Spezialfälle

- Notfallzugriff: Gesundheitsfachpersonen ohne Zugriffsrecht können im Notfall auf das EPD zugreifen.
  - Standardmässig können sie normal zugängliche Dokumente abrufen.
  - Patienten können diese Einstellung ändern, indem Sie auch eingeschränkt zugängliche Dokumente freigeben oder aber den Notfallzugriff grundsätzlich ausschliessen.
- Ausschluss: Patientinnen können verlangen, dass bestimmte Dokumente nicht in Ihrem EPD erfasst werden, oder können bereits abgelegte Dokumente wieder selbst löschen.
- Widerruf der Einwilligung: Patienten können ihre Einwilligung für das EPD jederzeit widerrufen; ihr EPD mit allen Dokumenten wird gelöscht.

Grenzen für die Datenanalyse

Die gesetzlich verankerte informationelle Selbstbestimmung setzt der Datenanalyse enge Grenzen, z.B.:

- Analysen müssen innerhalb eines Behandlungskontextes erfolgen
- Analysen müssen durch Gesundheitsfachpersonen oder deren Hilfspersonen, Patienten oder deren Stellvertreter erfolgen.
  - Andere Personengruppen (Forscher, Versicherer, Medizinalgerätehersteller, Pharmaindustrie…) sind ausgeschlossen
- Zugriffsrechte müssen explizit durch die Patienten erteilt werden.
  - Querschnittsanalysen über bedeutende Teile der Bevölkerung sind damit praktisch ausgeschlossen.

Es gibt im EPD keine Hintertüre für direkten Datenzugriff!

Chancen für die Datenanalyse

Die Analyse der im EPD abgelegten Daten wird Leben retten

- *Beispiel:* Die Austauschformate eMedikation ermöglichen eine vollständige Übersicht über die aktuelle Medikation eines Patienten und damit das Erkennen von Unverträglichkeiten

Die Analyse der EPD Daten wird neue Betreuungskonzepte ermöglichen

- *Beispiel:* Case Manager benötigen Daten aus unterschiedlichen Gesundheitseinrichtungen in einer für sie brauchbaren Form

Die zeitlich unbegrenzte Aufbewahrung der Dokumente im EPD ermöglicht Langzeitanalysen und fundiertere Beurteilungen

- *Beispiel:* eImpfausweis im EPD, geführt ab dem Kleinkindalter

Zugangsvarianten auf das EPD (1/2)

„Heute“ verfügbar: Zugang über Browser

- Patienten-Portal der Stammgemeinschaft (für Patienten und deren Stv.)
- GFP-Portal der Gemeinschaft (für GFP und deren Hilfspersonen)
- Internes GFP-Portal einer Gesundheitseinrichtung (falls implementiert)

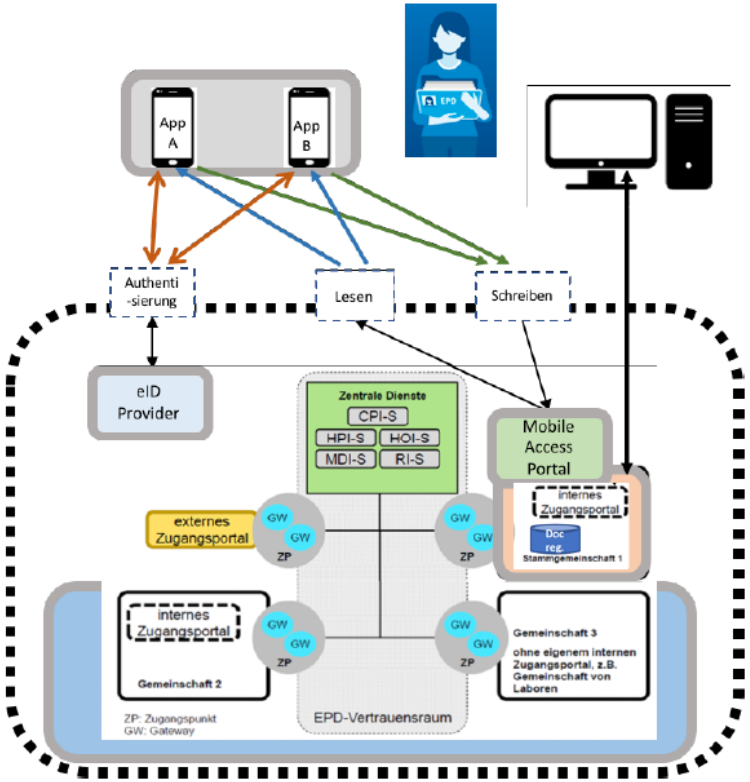
„Morgen“ verfügbar: Zugang über M2M-integrierte Anwendungen

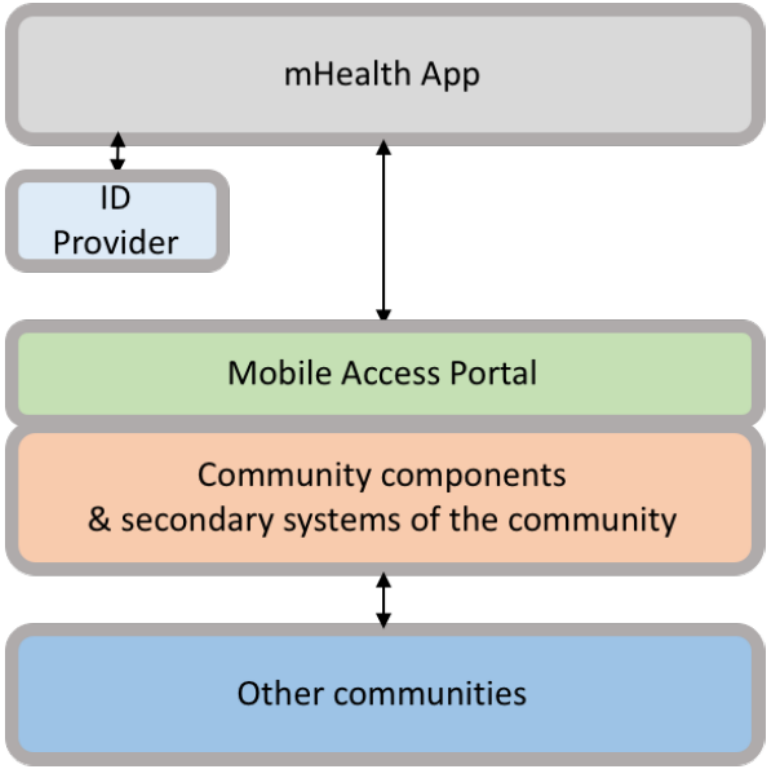
- Internes Klinik-Informationssystem (KIS) der Gesundheitseinrichtung
- Praxisinformationssystem (PIS) bei niedergelassenen Ärzten

Zugangsvarianten auf das EPD (2/2)

„Übermorgen“ verfügbar:

- Zugang über Apps





Quelle: “Grobkonzept Anbindung von mobilen Devices ans EPD” (eHealth Suisse und ahdis, 2019) (URL)

Technische Herausforderungen

- Analysewerkzeuge müssen mit den EPD Datenformaten umgehen können
  - Kurzfristig: Unstrukturierte Daten (insb. PDF)
  - Längerfristig: Strukturierte Daten gemäss EPD Austauschformaten
- Analysewerkzeuge müssen an die EPD-Portale angebunden werden
  - Nutzung von IHE- und/oder FHIR-Integrationsprofilen (derzeit in Entwicklung)
  - Integration mit zertifizierten Identity Providern über OpenID Connect (eID)

Schlusswort

- Das EPD revolutioniert das Gesundheitswesen (falls es die Durststrecke der ersten Jahre überlebt)
- Die Zusammenführung qualitativ hochwertiger Daten im EPD schafft für Gesundheitsfachpersonen und Patientinnen neue Analysemöglichkeiten bzw. Analysebedürfnisse
- Das EPD wird patientenzentrierte neue Dienstleistungen und Berufsgruppen schaffen, die ebenfalls einen legitimen Bedarf nach anwendungsgerechten Analysewerkzeugen haben

- Das EPD ist KEIN Selbstbedienungsladen für Datenkraken!

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch