Cybersecurity im ePD

Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV)

eHealth Forum Schweiz
09./10. März 2017

Thomas Kessler
Dipl. Physiker ETH
Gründer und Geschäftsführer TEMET AG

Agenda

- Einleitung
  - Vorstellung TEMET AG
  - Vorstellung ePD Modellversuch NWCH
- AKV und Risiko-Ownership: Ergebnisse der Analyse
  - Ziele und Vorgehen
  - Systemübersicht («Big Picture»)
  - RACI-Tabellen für die wichtigsten Anwendungsfälle
  - Risiko-Ownership *(im Referat nicht behandelt)*
- Schlussbemerkungen

Der Bericht «AKV und Risiko-Ownership für Informationssicherheit» wird, nach Fertigstellung voraussichtlich im Mai 2017, vom GDBS auch anderen interessierten Gemeinschaften zur Verfügung gestellt.

RACI: Responsible / Accountable / Consult / Inform
GDBS: Gesundheitsdepartement Basel-Stadt

Angaben zum Referenten Thomas Kessler

- Dipl. Physiker ETH, MAS ZFH in BA
- 26 Jahre Tätigkeit in der Informationssicherheit
  - 6 Jahre Fachstelle IT-Security bei einer Grossbank
  - 3 Jahre Leiter Security Engineering bei einem Finanzdienstleister
  - 17 Jahre IT-Security Beratung bei Finanzinstituten und Verwaltung
    - Davon 2 Jahre mit Fokus ePD
- Geschäftsführender Partner TEMET AG
  - Firmengründung im 2010
- Persönliche Schwerpunkte
  - IT-Sicherheitsarchitektur
  - Identity Provider (IdP)
  - Identity and Access Management (IAM)

thomas.kessler@temet.ch
079 508 25 43
www.temet.ch

Einleitung
TEMET AG

- Gründung: März 2010
- Inhabergeführte Aktiengesellschaft
- Sitz am Basteiplatz 5, im Herzen von Zürich
- Aktuell 12 Information Security Consultants
- Aktuell 71 Kunden aus Finanz, Verwaltung, Kritische Infrastrukturen und Gesundheitswesen

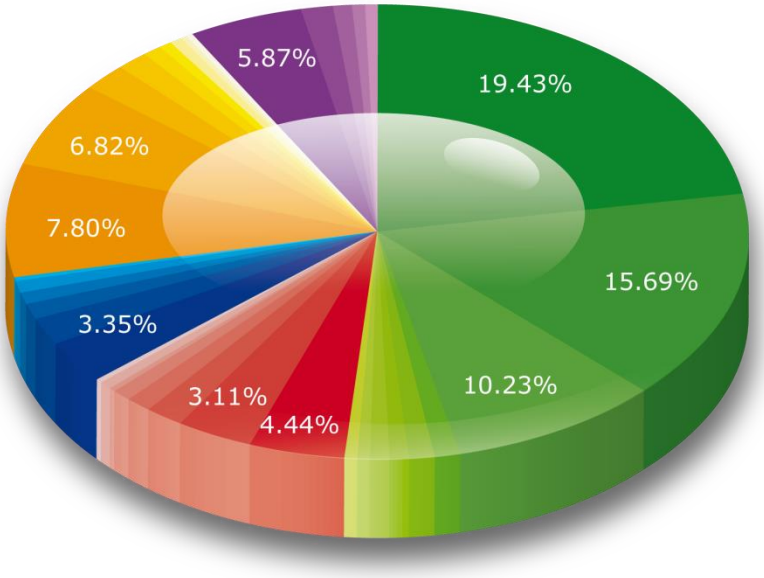
- Wir planen, konzipieren und realisieren Projekte für Informationssicherheit

Einleitung

Temet Kernkompetenzen

Einleitung

Temet Kundensegmente



Branchenverteilung Kunden
(Stand Juli 2016)

- Banken
- Verwaltung
- Versicherer
- Kritische Infrastrukturen
- Gesundheitswesen

(Segmente und Prozentzahlen entsprechen einzelnen Kunden)

Gesundheitswesen (11)	Bundesamt für Gesundheit BAG, Centris, CONCORDIA, Die Post – Vivates E-Health, Gesundheitsdepartement des Kantons Basel Stadt GDBS, Groupe Mutuel, Innova Versicherungen, Inselspital Bern, Novartis, Universitätsspital Zürich, Visana

Einleitung
eHealth Nordwestschweiz

- Initiative zur Implementierung und Weiterentwicklung von eHealth in der NWCH
- Gründung des Trägervereins eHealth NWCH mit dem Ziel, eHealth den Leistungserbringern zu übergeben
- Der Trägerverein hat drei Ziele (gemäss Statuten):
  - Durchführung des ePD-Modellversuchs in BS, erste EPDs zu Beginn 2018
  - Zertifizierung des ePD-Modellversuchs und somit Gründung einer Stammgemeinschaft gemäss EPDG im Verlaufe 2019
  - Parallele Entwicklung und Einführung von Mehrwertdiensten auf Basis der ePD-Infrastruktur (hybride Nutzung), im Speziellen Nutzung der Stammdaten

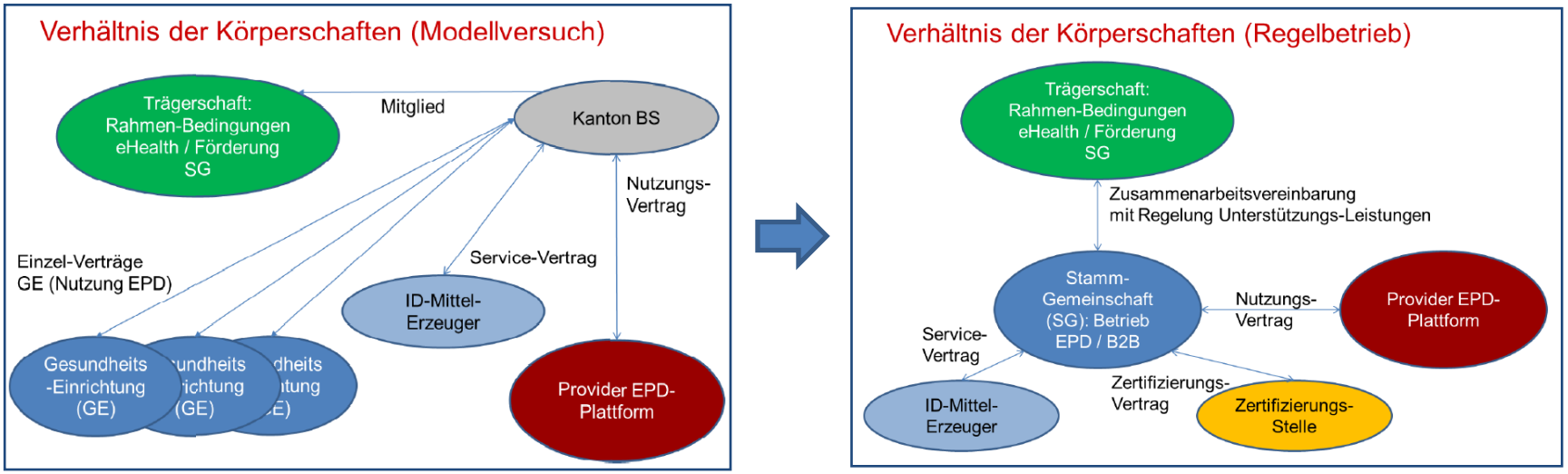
AKV Definitionen

Ausgangslage

- Gesetzesgrundlagen liegen (im Entwurf) vor
  - Baselstädtische eHealth-Verordnung (in Kraft seit Mai 2016)
  - Überarbeitete EPDV und TOZ im April 2017 erwartet
  - Wenig bzw. unscharfe Vorgaben bzgl. AKV innerhalb Gemeinschaften
- ePD-Modellversuch NWCH mit diversen Akteuren:
  - Gesundheitsdepartement Kanton Basel-Stadt (GDBS) als systemverantwortliche Institution (Dateneigner)
  - Verschiedene Gesundheitseinrichtungen (GE)
  - Betreiber ePD Plattform (Swisscom eHealth)
  - IdP für Patienten (Swisscom Passeport) und GFP (HIN)
- Vertragliche Vereinbarungen zwischen den Akteuren erfordern Klärung wichtiger AKV

AKV Definitionen
Zielsetzungen

- Identifikation kritischer Aktivitäten
- Risikobetrachtung
- Definition der AKV für den ePD-Modellversuch im Hinblick auf den zukünftigen Regelbetrieb



AKV Definitionen
Vorgehensweise

- RACI Tabelle pro Anwendungsfall
  - Identifizieren der wesentlichen Aktivitäten
  - Zuweisen der Verantwortlichkeiten an die Akteure
- RACI Definitionen (Auszug Wikipedia):

- **Responsible** – verantwortlich (Durchführungsverantwortung), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (auch durch Andere) gibt. Sie kann die Aktivität auch selbst durchführen. Wird auch als Verantwortung im disziplinarischen Sinne interpretiert.
- **Accountable** – rechenschaftspflichtig (Kosten-, bzw. Gesamtverantwortung), verantwortlich im Sinne von „genehmigen", „billigen" oder „unterschreiben". Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt. Wird auch als Verantwortung aus Kostenstellensicht interpretiert.
- **Consulted** – konsultiert. Eine Person, die vielleicht nicht direkt an der Umsetzung beteiligt ist, aber relevante Informationen für die Umsetzung hat und deshalb befragt werden soll oder muss, oder die eigentliche Arbeit ausführt (entspricht dann dem **Work** im REWA Konzept).
- **Informed** – zu informieren (Informationsrecht). Eine Person, die Informationen über den Verlauf bzw. das Ergebnis der Tätigkeit erhält oder die Berechtigung besitzt, Auskunft zu erhalten.

Quelle: Wikipedia (eingesehen im Januar 2017)

RACI Tabellen
Akteure

- Stammgemeinschaft (SG)
  - Im Modellversuch: Gesundheitsdepartement Basel-Stadt
- Gesundheitseinrichtungen (GE)
  - z.B Universitätsspital Basel, Felix Platter Spital
- Betreiber ePD Plattform
  - Im Modellversuch NWCH: Swisscom Health AG
- Identity Provider
  - Für Patientinnen und Patienten: Swisscom Passeport
  - Für GFP und HIP: z.B. HealthInfoNet AG
- Gesundheitsfachpersonen und Hilfspersonen
- Patientinnen und Patienten

GDBS: Gesundheitsdepartement Basel-Stadt / NWCH: Nordwestschweiz

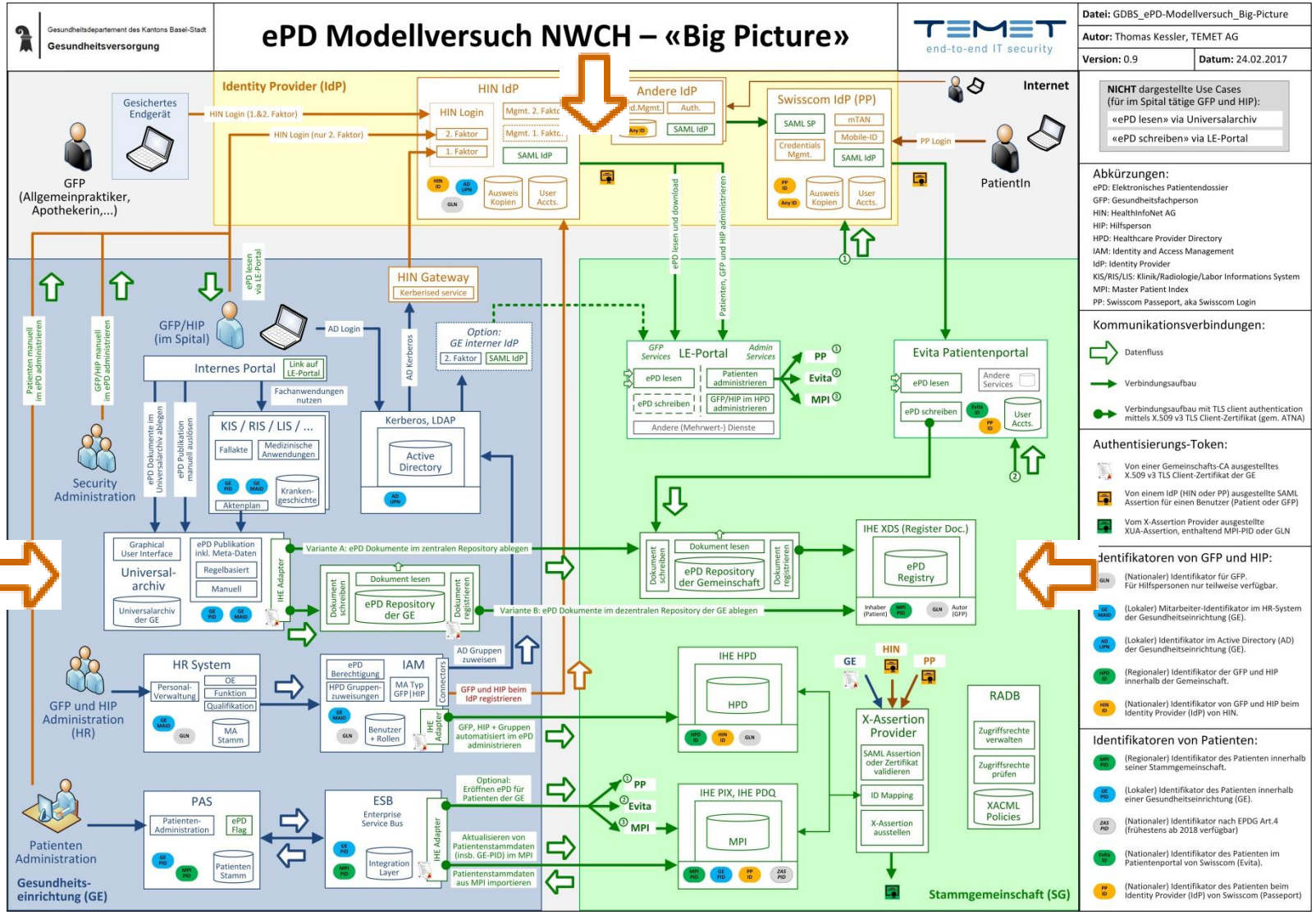
RACI Tabellen

Anwendungsfälle

- UC-1: ePD lesen
- UC-2: ePD schreiben
- UC-3: Patienten authentisieren
- UC-4: GFP und HIP authentisieren
- UC-5: Zugriffsrechte verwalten
- UC-6: Patientinnen und Patienten verwalten
- UC-7: GFP und HIP verwalten
- UC-8: Gesundheitseinrichtungen verwalten
- UC-9: Systeme betreiben
- UC-10: ISMS und DSMS betreiben

GFP: Gesundheitsfachperson / HIP: Hilfsperson
ISMS: Information Security Management System / DSMS: Datenschutz Management System

«Big Picture»


ePD Modellversuch NWCH – «Big Picture»
Gesundheitsdepartement des Kantons Basel-Stadt
Gesundheitsversorgung
end-to-end IT security
Datei: GDBS_ePD-Modellversuch_Big-Picture
Autor: Thomas Kessler, TEMET AG
Version: 0.9
Datum: 24.02.2017
Identity Provider (IdP)
HIN IdP
Andere IdP
Swisscom IdP (PP)
Internet
Gesichertes Endgerät
GFP (Allgemeinpraktiker, Apothekerin,...)
PatientIn
HIN Login (1.&2. Faktor)
HIN Login (nur 2. Faktor)
PP Login
NICHT dargestellte Use Cases (für im Spital tätige GFP und HIP):
«ePD lesen» via Universalarchiv
«ePD schreiben» via LE-Portal
Abkürzungen:
ePD: Elektronisches Patientendossier
GFP: Gesundheitsfachperson
HIN: HealthInfoNet AG
HIP: Hilfsperson
HPD: Healthcare Provider Directory
IAM: Identity and Access Management
IdP: Identity Provider
KIS/RIS/LIS: Klinik/Radiologie/Labor Informations System
MPI: Master Patient Index
PP: Swisscom Passeport, aka Swisscom Login
HIN Gateway
Kerberised service
GFP/HIP (im Spital)
AD Login
Option: GE interner IdP
Internes Portal
Link auf LE-Portal
Fachanwendungen nutzen
KIS / RIS / LIS / ...
Fallakte
Medizinische Anwendungen
Aktenplan
Kranken-geschichte
Kerberos, LDAP
Active Directory
Security Administration
LE-Portal
ePD lesen
ePD schreiben
Patienten administrieren
GFP/HIP im HPD administrieren
Andere (Mehrwert-) Dienste
Evita Patientenportal
Andere Services
User Accts.
Kommunikationsverbindungen:
Datenfluss
Verbindungsaufbau
Verbindungsaufbau mit TLS client authentication mittels X.509 v3 TLS Client-Zertifikat (gem. ATNA)
Authentisierungs-Token:
Von einer Gemeinschafts-CA ausgestelltes X.509 v3 TLS Client-Zertifikat der GE
Von einem IdP (HIN oder PP) ausgestellte SAML Assertion für einen Benutzer (Patient oder GFP)
Vom X-Assertion Provider ausgestellte XUA-Assertion, enthaltend MPI-PID oder GLN
Identifikatoren von GFP und HIP:
(Nationaler) Identifikator für GFP. Für Hilfspersonen nur teilweise verfügbar.
(Lokaler) Mitarbeiter-Identifikator im HR-System der Gesundheitseinrichtung (GE).
(Lokaler) Identifikator im Active Directory (AD) der Gesundheitseinrichtung (GE).
(Regionaler) Identifikator der GFP und HIP innerhalb der Gemeinschaft.
(Nationaler) Identifikator von GFP und HIP beim Identity Provider (IdP) von HIN.
Identifikatoren von Patienten:
(Regionaler) Identifikator des Patienten innerhalb seiner Stammgemeinschaft.
(Lokaler) Identifikator des Patienten innerhalb einer Gesundheitseinrichtung (GE).
(Nationaler) Identifikator nach EPDG Art.4 (frühestens ab 2018 verfügbar)
(Nationaler) Identifikator des Patienten im Patientenportal von Swisscom (Evita).
(Nationaler) Identifikator des Patienten beim Identity Provider (IdP) von Swisscom (Passeport)
ePD lesen via LE-Portal
ePD lesen und download
Patienten, GFP und HIP administrieren
Patienten manuell im ePD administrieren
GFP/HIP manuell im ePD administrieren
ePD Dokumente im Universalarchiv ablegen
ePD Publikation manuell auslösen
Universal-archiv
Graphical User Interface
ePD Publikation inkl. Meta-Daten
Regelbasiert
Manuell
Universalarchiv der GE
IHE Adapter
Variante A: ePD Dokumente im zentralen Repository ablegen
Dokument schreiben
Dokument lesen
ePD Repository der GE
Dokument registrieren
Variante B: ePD Dokumente im dezentralen Repository der GE ablegen
ePD Repository der Gemeinschaft
IHE XDS (Register Doc.)
ePD Registry
HR System
Personal-Verwaltung
OE
Funktion
Qualifikation
MA Stamm
GFP und HIP Administration (HR)
IAM
ePD Berechtigung
HPD Gruppen-zuweisungen
MA Typ GFP|HIP
Benutzer + Rollen
Connectors
AD Gruppen zuweisen
GFP und HIP beim IdP registrieren
GFP, HIP + Gruppen automatisiert im ePD administrieren
IHE HPD
HPD
GE
HIN
PP
X-Assertion Provider
SAML Assertion oder Zertifikat validieren
ID Mapping
X-Assertion ausstellen
RADB
Zugriffsrechte verwalten
Zugriffsrechte prüfen
XACML Policies
PAS
Patienten-Administration
ePD Flag
Patienten Stamm
Patienten Administration
Gesundheits-einrichtung (GE)
ESB
Enterprise Service Bus
Integration Layer
Optional: Eröffnen ePD für Patienten der GE
Aktualisieren von Patientenstammdaten (insb. GE-PID) im MPI
Patientenstammdaten aus MPI importieren
IHE PIX, IHE PDQ
MPI
Evita
Stammgemeinschaft (SG)

RACI Tabellen
Vorbemerkungen (1/2)

- Die nachfolgenden RACI-Tabellen basieren auf dem aktuellen Stand der Prozessdefinitionen
  - Im Projektverlauf sind Anpassungen zu erwarten
- Im Fokus der Prozesse und des «Big Picture» stehen (grössere) Gesundheitseinrichtungen
  - Andere (kleinere) Teilnehmer nur am Rande betrachtet
- Eine besondere Herausforderung sind die organisationsübergreifenden Prozesse für die Benutzerverwaltung (Patienten und GFP/HIP)
  - Effizienz, Sicherheit und Benutzerfreundlichkeit müssen unter einen Hut gebracht werden
  - Zusammenspiel zwischen GE, IdP und ePD Plattform
  - Solche Lösungen sind noch kaum erprobt

GE: Gesundheitseinrichtung / IdP: Identity Provider

RACI Tabellen
Vorbemerkungen (2/2)

- Das Referat fokussiert auf ausgewählte Punkte
  - Details können (später) nachgelesen werden
- Schwerpunkt auf den Verantwortlichkeiten für sicherheitsrelevante Prozesse und Aktivitäten
  - Benutzerverwaltung (Patienten und GFP/HIP)
  - Benutzerauthentisierung
  - Datenspeicherung
  - Sicherheitsmanagement
- Hinweis auf zwei spezielle AKV-Problematiken:
  1. Unsichere (z.B. private) Endgeräte von GFP/HIP
  2. Mehrfachanstellungen von GFP/HIP, speziell in der Kombination mit Gruppen-Zugriffsrechten

RACI Tabellen (1/10)

UC-1: ePD lesen (über LE-Portal und Patientenportal) – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Benutzer authentisieren	*Siehe Anwendungsfälle UC-3 (Authentisierung von Patienten) und UC-4 (Authentisierung von GFP/HIP)*					
Dossier auswählen *Anhand von Patientenidentifikatoren und demographischen Daten das richtige Dossier suchen und wählen*	-	-	-	-	A,R	A,R (nur eigenes Dossier)
Dokumente anzeigen *Alle im Dossier abgelegten Dokumente inkl. Meta-Daten übersichtlich anzeigen und bereitstellen*	-	-	A,R	-	-	-
Dokumente auswählen *Alle für den Behandlungskontext relevanten Dokumente auswählen*	-	-	-	-	A,R	A,R (nur eigene Dokumente)
Zugriffsrechte prüfen *Überprüfen, dass der Zugriff auf die gewünschten Dokumente erlaubt ist*	-	-	A,R	-	-	-
Fallakte ergänzen *Alle für den Behandlungskontext relevanten Dokumente ins Universalarchiv kopieren und mit den Fallakten verlinken*	-	-	-	-	A,R	-
Lokale Kopien sicher speichern *Die aus dem ePD kopierten Dokumente sicher speichern und soweit nötig aufbewahren*	1	A,R	-	-	-	A,R (nur eigene Dokumente)

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

Spezielle AKV Problematiken (1/2)

Private Endgeräte von GFP

- Gesundheitseinrichtungen sind für die Sicherheit von Patientendaten verantwortlich, die von ihren Mitarbeitenden bearbeitet werden
  - Spitäler investieren erhebliche Mittel in die Sicherheit der Arbeitsplatzumgebungen von GFP und HIP, insb.:
  - Sichere Endgeräte (z.B. Virenschutz, Local Firewall, restriktive lokale Rechte, Softwareverteilung,…)
  - Sichere Internet-Anbindung (z.B. Inhaltskontrolle und Sperrlisten auf E-Mail Gateway und Surf-Proxy,…)
- Die GE können aber selber nicht verhindern, dass GFP und HIP mit unkontrollierten eigenen Geräten auf das ePD zugreifen
  - Hierfür stehen die Identity Provider (IdP) in der Pflicht

RACI Tabellen (2a/10)

UC-2: ePD schreiben (über M2M Kommunikation) – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Datenquelle authentisieren *Sicherstellen, dass es sich um eine an der Gemeinschaft teilnehmende Gesundheitseinrichtung handelt.*	-	C	A,R Validieren TLS Client-Zertifikat der GE	-	-	*vgl. UC-3 (Authentisierung von Patienten)*
Dossier auswählen *Anhand von Patientenidentifikatoren und demographischen Daten das richtige Dossier suchen und wählen*	-	A,R	-	-	-	A,R (nur eigenes Dossier)
Ausschluss prüfen *Sicherstellen, dass die Behand-lungsepisode nicht vom ePD ausgeschlossen wurde*	-	A,R	-	-	-	-
Dokumente identifizieren *Alle behandlungsrelevanten Doku-mente gemäss Regelwerk der GE automatisch auswählen*	-	A,R	-	-	-	-
Zusatzdokumente auswählen *Zusätzliche behandlungsrelevante Dokumente manuell auswählen*	-	A,I	-	-	R	A,R (nur eigene Dokumente)

...

RACI Tabellen (2b/10)

UC-2: ePD schreiben (über M2M Kommunikation) – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
...						
Datenkonformität sicherstellen *Sicherstellen, dass die Dokumente in einem zulässigen Datenformat vorliegen und keine Schadsoftware enthalten (Virenscan).*	-	A,R	-	-	-	-
Dokumente im ePD ablegen *Selektierte Dokumente ins ePD Repository kopieren und Meta-Daten in der ePD Registry erfassen*	-	A,R	C Daten ent-gegennehmen	-	-	-
Sichere ePD Datenablage *Die im ePD Repository abgelegten Dokumente sicher speichern und soweit nötig aufbewahren*	-	A,R (dezentrales PD Repository)	A,R (zentrales ePD Repository)	-	-	-
Dokumente aus ePD löschen *Ausgewählte im ePD Repository abgelegte Dokumente löschen*	-	-	A,R (bei Aufhebung des ePD z.B. im Todesfall)	-	-	A,R

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (3/10)

UC-3: Patienten authentisieren – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	Swisscom (PP)	-	-
Qualitätsvorgaben definie - *Angebotene 2-FA Verfahren* - *Passwortregeln (Länge, Komplexität, Zeichensatz, Lebensdauer,...)* - *Session Timeouts* - *Umgang mit Fehlversuchen*	A (Modellversuch) I (Regelbetrieb)	-	-	R (Modellversuch) A,R (Regelbetrieb)	-	I
Zwei Faktoren prüfen *Aktuell zwei Verfahren verfügbar:* *V1: Passwort + SMS OTP (mTAN)* *V2: Passwort + Mobile-ID (M-ID)*	-	-	-	A,R	-	C
SAML Assertion ausstellen *Ausstellen der SAML Assertion zu Handen des Patientenportals (Evita)*	-	-	-	A,R	-	-
SAML Assertion prüfen *Validieren der SAML Assertion, bevor der ePD-Zugang erlaubt und eine XUA Assertion ausgestellt wird*	-	-	A,R	-	-	-
XUA Assertion ausstellen *Ausstellen der XUA Assertion zu Handen der ePD Zugriffskontrolle, ggf. Mapping PP-ID auf MPI-PID*	-	-	A,R	-	-	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (4a/10)

UC-4: GFP und HIP authentisieren – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN (Ofac)	-	-
Qualitätsvorgaben definieren - *Angebotene 2-FA Verfahren* - *Passwortregeln (Länge, Komplexität, Zeichensatz, Lebensdauer,...)* - *Session Timeouts* - *Umgang mit Fehlversuchen*	A (Modellversuch) I (Regelbetrieb)	-	-	R (Modellversuch) A,R (Regelbetrieb)	I	-
Endgerät prüfen *Prüfen, dass ein kontrolliertes (z.B. GE domänenintegriertes) Endgerät genutzt wird*	-	C	-	A,R	-	-
Ersten Faktor prüfen *Passwortprüfung*	-	R AD Passwort falls genutzt	-	A,R IdP Passwort falls genutzt	C	-
Zweiten Faktor prüfen *Unterschiedlich je nach unterstützten Verfahren (noch nicht definiert)*	-	-	-	A,R	C	-

...

RACI Tabellen (4b/10)

UC-4: GFP und HIP authentisieren – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN (Ofac)	-	-
...						
SAML Assertion ausstellen *Ausstellen der SAML Assertion zu Handen des LE-Portals*	-	-	-	A,R	-	-
SAML Assertion prüfen *Validieren der SAML Assertion, bevor der ePD-Zugang erlaubt und eine XUA Assertion ausgestellt wird*	-	-	A,R	-	-	-
XUA Assertion ausstellen *Ausstellen der XUA Assertion zu Handen der ePD Zugriffskontrolle, ggf. Mapping IdP-ID auf GLN*	-	-	A,R	-	-	-
Absichern Notfallzugriff *Re-Authentisieren der GFP vor jedem Notfallzugriff*	-	-	A,R Re-Authentisierung auslösen	R Re-Authentisierung durchführen	C	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (5a/10)

UC-5: Zugriffsrechte verwalten – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Grundeinstellung festlegen	*Die Grundeinstellung der Zugriffsrechte und Vertraulichkeitsstufen wird vom Bundesrat festgelegt*					
Grundeinstellung anpassen - *Zugriffsrechte auf 6 Mt. befristen* - *Notfallzugriff einschränken, erweitern oder ausschliessen* - *Minimale Vertraulichkeitsstufe neuer Dokumente anpassen* - *Automatismus für Rechtezuteilung an neue GFP Gruppenmitglieder deaktivieren*	-	-	-	-	-	A,R
Vertraulichkeitsstufe setzen *Vertraulichkeitsstufe neu eingestellter Dokumente gemäss Grundeinstellung oder höher erfassen*	-	A,R	-	-	-	-
Vertraulichkeitsstufe anpassen *Vertraulichkeitsstufe von Dokumenten nach eigenem Ermessen anpassen*	-	-	-	-	-	A,R
Zugriffsrechte erteilen *Zugriffsrechte an GFP und Gruppen von GFP erteilen*	A (GFP Gruppen-Konzepte)	R (GFP Gruppen-bildung)	-	-	-	A,R

...

RACI Tabellen (5b/10)

UC-5: Zugriffsrechte verwalten – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
...						
Ausschlussliste pflegen *Gesundheitsfachpersonen auf die Ausschlussliste setzen*	-	-	-	-	-	A,R
GFP ermächtigen *GFP dazu ermächtigen, eigene Zugriffsrechte weiterzugeben*	-	-	-	-	I	A,R
Zugriffsrechte weitergeben *Eigene Zugriffsrechte an GFP und Gruppen von GFP weitergeben*	-	-	-	-	A,R (sofern ermächtigt)	-
Stellvertreter benennen *Beliebige (mit einem Identifikationsmittel ausgestattete) Personen dazu berechtigen, unter der eigenen MPI-PID das ePD zu nutzen*	-	-	-	-	-	A,R

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (6a/10)

UC-6: Patienten verwalten (mit GE als „one-stop-shop") – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	Swisscom (PP)	-	-
Qualitätsvorgaben definieren - *Aktualisierungsfristen für die verschiedenen Verzeichnisse* - *Regelung für das MPI-Clearing* - *Aufbewahrungsfristen* - *Vorgaben für Patientenaufklärung*	A,R	C	-	-	-	-
Patientin identifizieren *Ausweis prüfen und scannen, evt. Passwortbrief und Aktivierungscode für ID-Mittel aushändigen,...*	-	R (im Auftrag des IdP)	-	A, C (beglaubigte Dokumente aufbewahren)	-	C Ziel: Einmalige Präsenz vor Ort („one-stop-shop")
ePD Onboarding *Patientin aufklären, Einwilligung einholen, prüfen und scannen,...*	A	R (im Auftrag der Gemeinschaft)	C (beglaubigte Dokumente aufbewahren)	-	-	
Patient in der Stamm-gemeinschaft registrieren *Eintrag (manuell oder elektronisch) im MPI der Gemeinschaft erfassen. MPI-Clearing für Eindeutigkeit.*	A	R (im Auftrag der Gemeinschaft)	C (Daten ent-gegennehmen)	-	-	I

...

RACI Tabellen (6b/10)

UC-6: Patienten verwalten (mit GE als „one-stop-shop") – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	Swisscom (PP)	-	-
...						
Registrieren (National) *Nationale Patientenidentifikations-nummer PID von ZAS beziehen [zukünftig]*	-	-	A,R	-	-	I
Registrieren (Patientenportal) *Evita-Benutzerkonto für den Patien-ten einrichten (sofern noch nicht vorhanden)*	-	I	A,R	-	-	C
Registrieren (Identity Provider) *Passeport-Identität für den Patien-ten einrichten (sofern noch nicht vorhanden)*	-	I	A	R	-	C
ID-Mittel zustellen *Zustellen/aktivieren der Authenti-sierungsmittel für den ePD-Login*	-	-	-	A,R	-	C
Abgleich mit PAS *Verknüpfen des MPI-Eintrags mit dem (korrekten!) Patienteneintrag bei der GE; laufende Aktualisierung.*	-	A,R	-	-	-	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (7a/10)

UC-7: Am Spital tätige GFP und HIP verwalten – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN	-	-
Qualitätsvorgaben definieren - *Aktualisierungsfristen für die verschiedenen Verzeichnisse* - *Aufbewahrungsfristen* - *Regeln für GFP Gruppenbildung*	A,R	C	-	-	-	-
GFP / HIP identifizieren - *Ausweis prüfen und scannen* - *GLN erfassen (ggf. beschaffen)* - *Passwortbrief und Aktivierungs-code für ID-Mittel aushändigen*	-	R (im Auftrag des IdP)	-	A, C (beglaubigte Dokumente aufbewahren)	-	-
Qualifikation prüfen *Qualifikationen prüfen (manuelle oder elektronische Registerabfrage)*	-	-	-	A, R (Register-Abfrage)	-	-
ePD Zugang autorisieren *Zugang zum ePD erteilen, z.B. anhand von Funktion oder OE-Zugehörigkeit bei der GE*	-	A,R	-	-	C	-
GFP/HIP im HPD registrieren *Eintrag mit Stammdaten im HPD der Gemeinschaft erfassen und pflegen, manuell oder über IAM*	-	A,R	C (Daten ent-gegennehmen)	(R) (Falls von der GE beauftragt)	I	-

...

RACI Tabellen (7b/10)

UC-7: Am Spital tätige GFP und HIP verwalten – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN	-	-
...						
HIP den GFP zuordnen *Im HPD erfassen und pflegen, welche Gesundheitsfachperson für eine Hilfsperson verantwortlich ist*		A,R	C (Daten ent-gegennehmen)	-	I	-
GFP Gruppen zuteilen *Im HPD erfassen und pflegen, welche GFP/HIP welchen Gruppen angehören*	2	A,R	C (Daten ent-gegennehmen)	-	I	-
Registrieren (Identity Provider) *HIN-Identität erfassen und pflegen, manuell oder über IAM*	-	A,R	-	C (Daten ent-gegennehmen)	I	-
ID-Mittel zustellen *Zustellen/aktivieren der Authenti-sierungsmittel für den ePD-Login*	-	(R) AD Passwort falls genutzt	-	A,R	C	-
Registrieren (nationales HPD) *Eintrag im nationalen HPD erfassen und pflegen (GFP, keine HIP) [zukünftig]*	-	I	A,R	-	I Nur GFP	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

Spezielle AKV Problematiken (2/2)

Mehrfachanstellungen

- Aus der Mehrfachanstellung von GFP/HIP in der Kombination mit Gruppen-Zugriffsrechten ergibt sich die folgende «AKV-Problematik»:
  - Patienten erteilen ein Gruppen-Zugriffsrecht (z.B. an Klinik «A») ggf. im Vertrauen darauf, dass ihre Daten den Verantwortungsbereich dieser Klinik nicht verlassen
  - Es ist möglich, dass eine GFP oder HIP gleichzeitig bei den Gesundheitseinrichtungen «A» und «B» in einem Anstellungsverhältnis steht («Mehrfachanstellung»)
  - Klinik «A» kann die Ausübung des Gruppen-Zugriffsrechts nicht kontrollieren, während die GFP oder HIP im Rahmen von Arbeitsvertrag «B» tätig ist

RACI Tabellen (8/10)

UC-8: Gesundheitseinrichtungen verwalten – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Teilnahmebedingungen *Festlegen der Bedingungen für die Teilnahme am Modellversuch*	A,R	C	C	C	C (via Standes-organisation)	C (via Patienten-organisation)
Entscheid über Aufnahme Prüfung der Einhaltung der Teil-nahmebedingungen	A,R	C	C	I	-	-
Anbindung der GE Technische und organisatorische Integration in die Gemeinschaft	I	A,R	C	C	-	-
Teilnehmerverzeichnis Führen eines aktuell gehaltenen Verzeichnisses aller Teilnehmer	A,R	I	C (technische Konfiguration)	I	I	I
Entscheid über Austritt Freiwilliger Austritt aus der Gemein-schaft	I	A,R	I	I	-	-
Entscheid über Ausschluss Ausschluss (ggf. befristet) einer Gesundheitseinrichtung aus der Gemeinschaft	A,R	C	I	I	-	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (9/10)

UC-9: Systeme betreiben – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Systeme bei der GE *Dezentrale ePD Repositories, Endgeräte von GFP und HIP, IHE Adapter.*	A	R	C (Schnittstellen)	C (Schnittstellen)	-	-
Systeme der Gemeinschaft *Zentrale ePD Repositories, Registry, MPI, HPD, Patientenportal, LE-Portal, X-Assertion Provider, RADB*	A	C (Schnittstellen)	R	C (Schnittstellen)	-	-
Identity Provider für Patie *Swisscom Passeport*	A (Modellversuch) I (Regelbetrieb)	-	C (Schnittstellen)	R (Modellversuch) A,R (Regelbetrieb)	-	I
Identity Provider für GFP/HIP *HIN IdP und HIN Gateway*	A (Modellversuch) I (Regelbetrieb)	R (HIN Gateway)	C (Schnittstellen)	R (Modellversuch) A,R (Regelbetrieb)	-	-
Endgeräte von Patienten *PC und Mobilgeräte mit Browser und Apps*	-	-	-	-	-	A,R

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

RACI Tabellen (10/10)

UC-10: ISMS und DSMS betreiben – RACI Tabelle

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
	a.i.: GDBS	USB, FPS,...	Swisscom	HIN & Swisscom	-	-
Identify *Steuerung und Kontrolle, insb.:* *- Aufbau und Betrieb des ISMS* *- ISDS-Verantwortlicher der SG* *- Security-Board der SG*	A,R	C	C	C	C (via Standes-organisation)	C (via Patienten-organisation)
Protect *Präventive Sicherheitsmassnahmen (Mensch, Technik, Organisation)*	A	R (eigene Systeme)	R (eigene [illegible])	R (Modellversuch) A,R (Regelbetrieb)	-	A,R (eigenes Endgerät)
Detect *Überwachung und Erkennung von Sicherheitsvorfällen bzgl. ePD (Security Operations Center SOC)*	A,I	I	R (alle ePD Services)	R (ePD Login)	-	A,R (eigenes Endgerät)
Respond *Reaktion auf Sicherheitsvorfälle inkl. Kommunikation intern und extern*	A,R	I	R (Sofortmass-nahme: Abschalten)	I	I (soweit direkt betroffen)	I (soweit direkt betroffen)
Recover *Wiederherstellung des Normalzu-stands und Verbesserung des Sicherheitsdispositivs*	A	R (eigene Systeme)	[illegible] Systeme)	A,R (eigene Systeme)	-	A,R (eigenes Endgerät)

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

Schlusswort

- Der ePD Vertrauensraum ist ein vielschichtiges Gebilde mit vielen gegenseitigen Abhängigkeiten
- Jede einzelne (Stamm-)Gemeinschaft ist in sich nochmals ein vielschichtiges Gebilde mit vielen gegenseitigen Abhängigkeiten
- Die zweckmässige Zuteilung der Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) an die Akteure ist ein wesentlicher Erfolgsfaktor
  - Die heute vorgestellten RACI-Tabellen können ggf. als Diskussionsbasis und Richtschnur genutzt werden

Der Bericht «AKV und Risiko-Ownership für Informationssicherheit» wird, nach Fertigstellung voraussichtlich im Mai 2017, vom GDBS auch anderen interessierten Gemeinschaften zur Verfügung gestellt.

Besten Dank für Ihre Aufmerksamkeit!

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