ELCA

eHealth Schweiz

Basisinfrastruktur
Konzeption der Basiskomponenten

Im Auftrag des Koordinationsorgans Bund-Kantone

Version 1.0 vom 9.4.2010

16.08.2010
ELCA Informatik AG, Steinstrasse 21, Postfach, CH-836 Zürich
T. Bähler, M. Demarmels, P. Paschke, T. Schaller, M. Schröder

Zweck und Positionierung dieses Dokuments

Die Analysen, Vorschläge und Empfehlungen in diesem Dokument sind das Resultat der Konzeptarbeit des Mandatnehmers im Dialog mit der Co-Leitung des Teilprojektes "Standards und Architektur". Sie richten sich an die Gremien von "eHealth Suisse" und dienen dort als Grundlage für die Diskussion im Hinblick auf die Verabschiedung von weiteren Empfehlungen. Diese Vorschläge können von den konsolidierten und verabschiedeten Empfehlungen von "eHealth Suisse" abweichen.

Management Summary

Dieses Dokument enthält Empfehlungen für die Konkretisierung/Ausgestaltung der Komponenten der Basisinfrastruktur eHealth Schweiz.

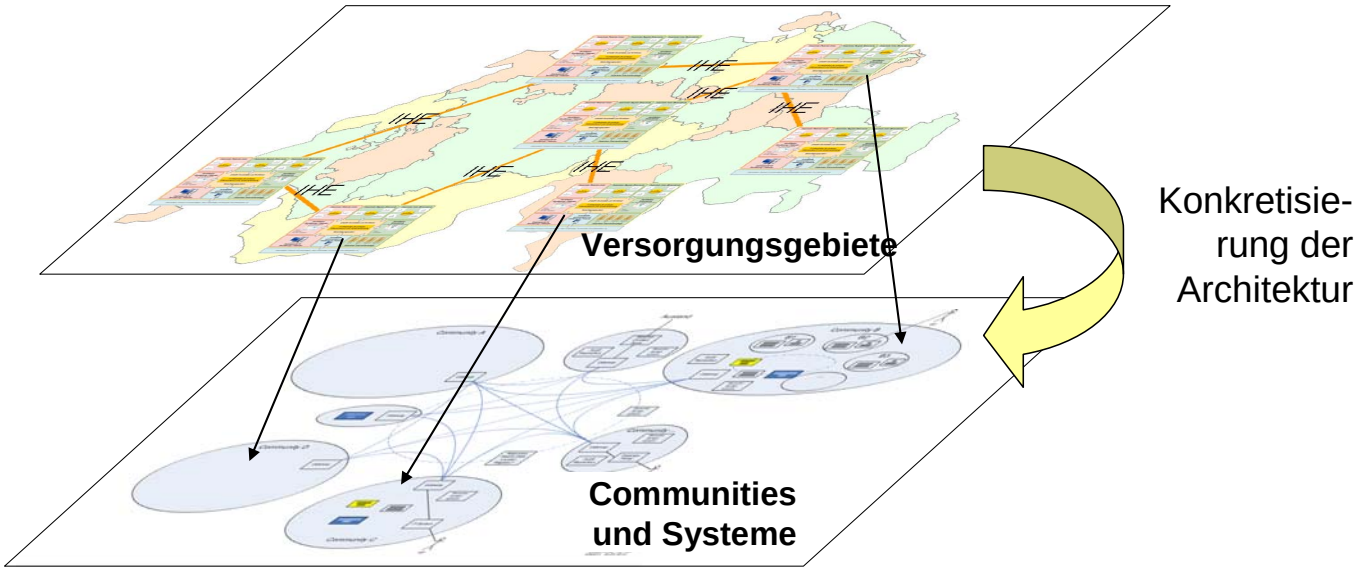
Die Inhalte dieses Dokumentes wurden im Rahmen eines Auftrages des Koordinationsorgans eHealth Bund-Kantone an die Firma ELCA Informatik AG durch ein Projektteam von Mitarbeitenden von ELCA, medshare und Lake Griffin und unter Begleitung des Koordinationsorgans in den Monaten Februar bis April 2010 erarbeitet.

Wie sieht das Gesamtbild des Systems „eHealth Schweiz“ aus?

Das Gesamtsystem besteht aus einer Menge von **Gemeinschaften / Communities**, welche jeweils lokale / bereichsspezifische Systeme enthalten: je nach Ausgestaltung Patientenindizes, Dokumentenregister/-ablagen, Behandelndenverzeichnisse und/oder Zugangsportale; weiter stellt eine Community mit dem National Contact Point den Austausch mit dem Ausland sicher.

Die Gemeinschaften/Communities sind mittels **Gateways („Eingangspforten“ / „Netzübergängen“)** und einer **IT-Infrastruktur** miteinander verbunden. Im so entstandenen Gesamtsystem sind Systeme übergreifend miteinander operabel und können Informationen austauschen. Dies erfolgt im Rahmen der jeweils bereitgestellten Funktionalitäten und Daten, sowie unter Berücksichtigung des noch zu definierenden Berechtigungskonzepts

Die folgende Abbildung visualisiert die Konkretisierung der Architektur aus der Perspektive der regionalen Versorgungsgebiete (für eine vollständigere Visualisierung wird an dieser Stelle auf Abbildung 1 auf Seite 9 verwiesen).



Die Tabelle auf der folgenden Seite gibt einen Überblick über die Ausgestaltung sowie die wesentlichen Standards und Design-Prinzipien der einzelnen Basiskomponenten. Punkte, welche noch nicht geklärt sind oder bei denen es Varianten gibt, sind mit „offen“ markiert.

Ausgestaltung der Basiskomponenten der Architektur

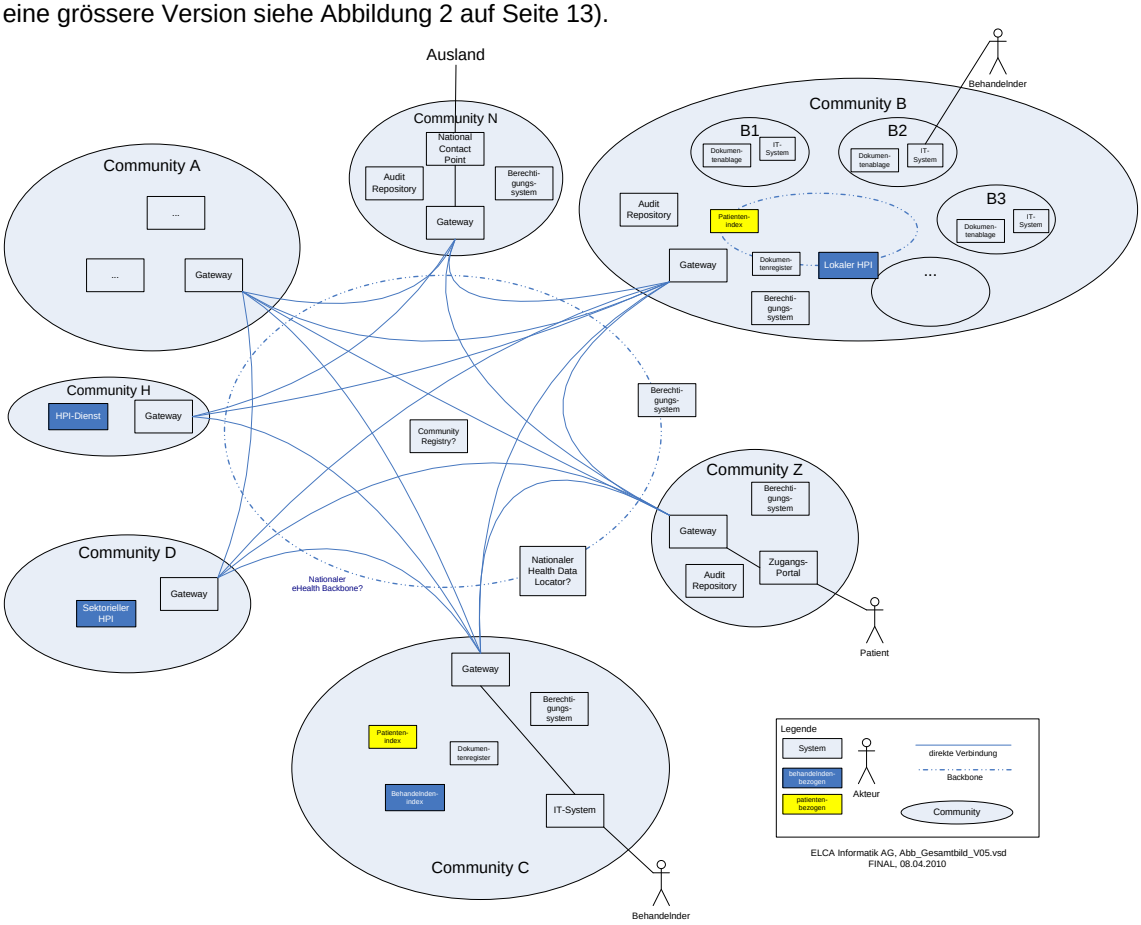
Basiskomponente (Kapitel)	Ausgestaltung	Standards / Design-Prinzipien
IT-Infrastruktur (Kap. 4)	Sichere Anbindung der Communities (via Gateways), Weiterleiten von Nachrichten und Sicherstellen der Transport Layer Security (TLS) Offen: Varianten Ausgestaltung – Zentrale Community Registry – eHealth Schweiz Backbone Offen: Optionale gemeinsame Funktionalitäten Verschiedene Funktionalitäten könnten statt in den Gateways Teil der IT-Infrastruktur sein.	• IHE ATNA - TLS - Gateways als Secure Nodes • Anbindung Communities via Gateways
Berechtigungssystem (Kap. 5)	Anforderungen: Authentisierung, Ausstellen und Auswerten Security Tokens, Durchsetzen Richtlinien und Policies, Verwaltung Berechtigung und Auditmöglichkeiten	• Anwendung bei allen Elementen der Architektur • IHE XUA (zwischen Communities) • Empfohlen innerhalb Communities: IHE EUA/XUA
Patientenindex (Kap. 6)	**Lokale Patientenindizes** als Teil der Communities Kein übergreifender CH-weiter Index Offen: genaue Merkmale Patienten Offen: Varianten Identifikation Patienten – eindeutiges Merkmal – in der Gesamtheit eindeutiges Merkmalsset	• Suche von Patienten via Community Gateways • IHE XCPD (Gateway) • Empfohlen innerhalb Communities: IHE PIX, PDQ
Index Behandelnde und Institutionen (Kap. 7)	**HPI[1]-Dienst** als zentraler Verzeichnisdienst für Abfrage von Behandelnden/Institutionen **Sektorielle HPIs** als führende Systeme für bereichsspezifische Verzeichnisse **Lokale HPIs** für lokale Bedürfnisse Offen: genaue Merkmale Behandelnde Offen: Identifikation Behandelnde – eindeutiges Merkmal – in der Gesamtheit eindeutiges Merkmalsset Offen: genaue Merkmale Institutionen Offen: Verknüpfung Behandelnde-Institutionen	• HPI-Dienst ist zentraler Zugangspunkt / Service und kein eigener Index • Offen: Integration mit sektoriellen HPIs
Dokumentenregister (Kap. 8)	**Lokale Dokumentenregister** als Teil der Communities Kein übergreifendes CH-weites Register	• Community-übergreifende Abfragen via Community Gateways • IHE XCA (zwischen Communities) • Empfohlen innerhalb Communities: IHE XDS oder direkt IHE XCA
Dokumentenablage (Kap. 9)	**Lokale Dokumentenablagen** als Teil der Communities Keine übergreifende CH-weite Ablage	• Zugriff auf Dokumente via Community Gateways • IHE XCA (zwischen und innerhalb der Communities)
Zugang (Kap. 10)	Ausgestaltung im Rahmen des Community-Konzeptes mit Gateways, Audit Repository und Berechtigungssystem	

In Ergänzung sind weitere Elemente nötig, welche die Zusammenfassung auf folgender Seite zeigt.

[1] HPI = Health Professional Index

Gesamtbild / Ausgestaltung der Communities

Die folgende Abbildung zeigt das Gesamtbild mit Communities und den wichtigsten Elementen (für eine grössere Version siehe Abbildung 2 auf Seite 13).



Auf nationaler Ebene gibt es:

- Ein Ensemble von „Communities“
- Eine IT-Infrastruktur, welche die Communities verbindet.
- Je nach Ausgestaltung weiter gehende Funktionalität, welche statt individuell in den Communities als gemeinsamer Teil der IT-Infrastruktur umgesetzt wird.

Communities können die folgenden Systeme enthalten:

- Community Gateway (zwingend)
- Audit-Repository (zwingend)
- Patientenindex
- Dokumentenregister
- Lokale Dokumentenablagen
- „Sektorielle HPIs“
- „Lokale HPIs“
- Zugangsportale
- Weitere „IT-Systeme“, welche mit den oben genannten Systemen integriert sind bzw. Daten liefern oder beziehen.

Je nach Ausgestaltung können Communities sehr viele dieser Elemente oder nur einzelne enthalten.

Im Gesamtsystem gibt es zwei besondere Communities:

- Eine Community, welche den gemeinsamen „HPI-Dienst“ enthält.
- Eine Community, welche dem national übergeordneten Austausch dient und den National Contact Point (NCP) für epSOS enthält.

Offene Punkte / nächste Schritte

Die folgenden offenen Punkte bzw. nächsten Schritte sind im Anschluss an die vorliegende Konkretisierung der Basiskomponenten anzugehen. Am Ende jedes Kapitels sind diese Punkte / Schritte jeweils kurz mit einigen Details erläutert.

Kap.	Offener Punkt / nächster Schritt
2	Spezifikation von Richtlinien für Communities (inkl. gesetzliche Grundlagen)
	Operationalisierung des Reifegradmodells
3	Illustration der Use cases anhand der Resultate aller drei Mandate (Basiskomponenten, Rollenkonzept, Metadaten) – eventuell auch gemeinsam mit Ausgestaltung des Berechtigungssystems
4	Wahl der grundlegenden Variante für die IT-Infrastruktur (nur zentrale Registry oder Backbone?)
	Konkretisierung weiter gehender gemeinsamer Funktionalität
	Analyse / Klärung der Performance des Gesamtsystems
5	Erstellen eHealth Governance
	Konzeption Berechtigungssystem
6	Identifikation Patient: Auswahl Variante
	Identifikation Patient: über CH hinaus / Ausland
7	Konkretisierung HPI-Dienst (fachliche Sicht)
	Konkretisierung HPI-Dienst (technische Sicht)
8	Spezifikation der CH-spezifischen Umsetzung der Dokumentenregister
10	Konkretisierung Szenarien Zugang (fachlich/technisch
	Erweiterung Rollenkonzept um weiteren Teilnehmerkreis

Daneben gibt es verschiedene Anforderung an die OID-Registrierung, welche in Kap. 2.4 aufgeführt sind.

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument enthält einen Vorschlag für die Konkretisierung/Ausgestaltung der Komponenten der Basisinfrastruktur eHealth Schweiz. Die Inhalte dieses Dokumentes wurden im Rahmen eines Auftrages des Koordinationsorgans eHealth Bund-Kanton an die Firma ELCA Informatik AG durch ein Projektteam von Mitarbeitenden von ELCA, medshare und Lake Griffin und unter Begleitung des Koordinationsorgans in den Monaten Februar bis April 2010 erarbeitet.

1.1 Kontext

Dieses Dokument liefert eine vertiefte Beschreibung der Inhalte der Basiskomponenten der Architektur eHealth Schweiz. Es stellt somit einen weiteren Konkretisierungsschritt der Ausgestaltung der eHealth-Strategie Schweiz dar. Die folgende Abbildung illustriert diesen Kontext.

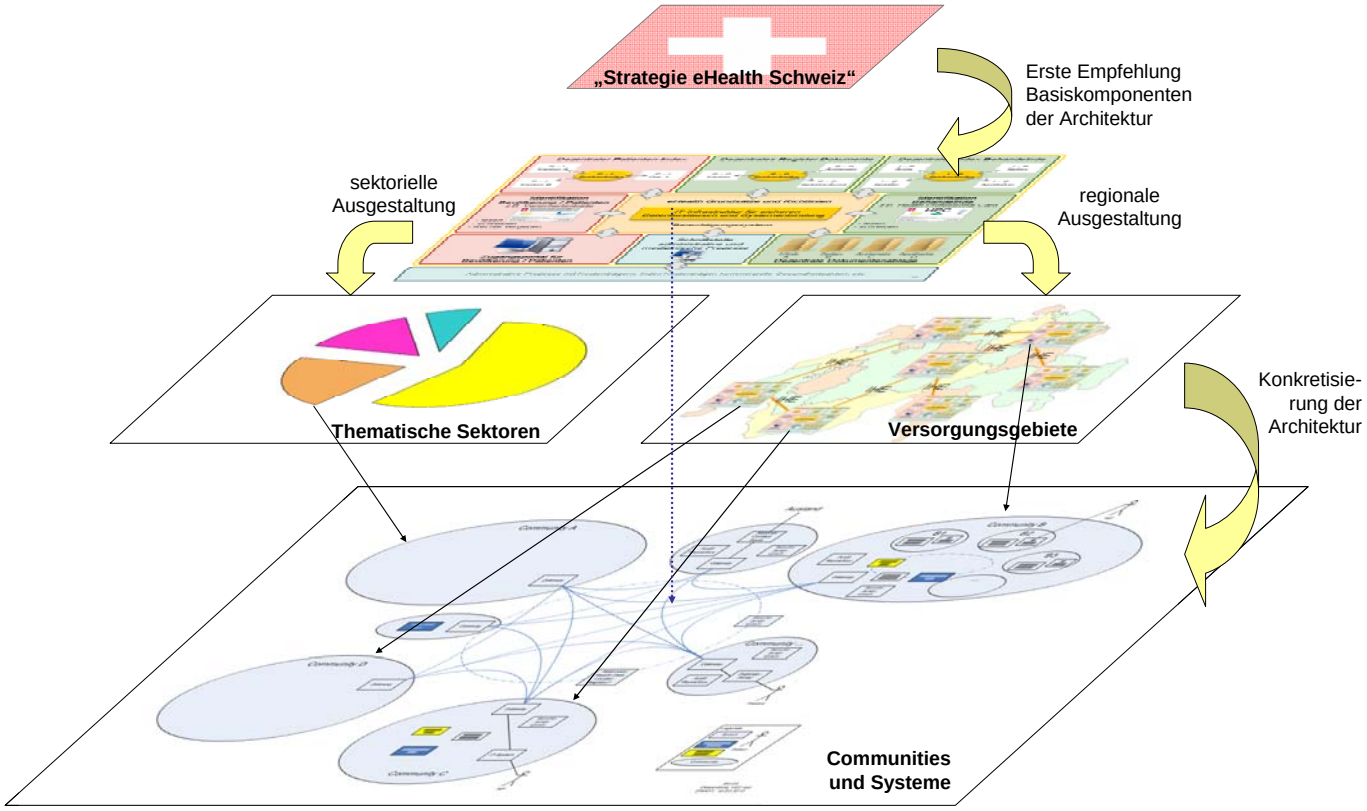


Abbildung 1: Kontext der vorliegenden Konzeption der Basiskomponenten (unterste Ebene)

1.2 Leitlinien, Grundsätze und Richtlinien

Die Vorarbeiten im TP Standards und Architektur definieren verschiedene Leitlinien, Grundsätze und Richtlinien:

- **Übergeordnete Leitlinien**
  Der Bericht „Empfehlung TP – Bericht für die Anhörung“ vom 19.3.09 definiert 11 Leitlinien auf übergeordneter Ebene
- **Grundsätze**
  Der Bericht „Standards und Architektur – Erste Empfehlungen“ vom 19.3.09 definiert 16 Grundsätze, welche bereits erste Implikationen für die Architektur enthalten.

- **Empfohlene Standards in der Startphase**
  Ebenfalls im Bericht „Standards und Architektur – Erste Empfehlungen“ vom 19.3.09 werden sehr konkrete architekturbezogene Vorgaben gemacht. Diese umfassen
  - prozessorientierte Standardisierung mit Anwendungsfällen basierend auf der IHE Initiative
  - Verwendung der Integrationsprofile XDS, PIX/PDQ, XUA und ebXML

1.3 Vorgehen

Das vorliegende Dokument wurde durch ein Kernteam unter Führung der Firma ELCA erarbeitet. Mitglieder dieses Kernteam waren:

- Thomas Bähler, ELCA
- Peter Paschke, ELCA
- Michael Schröder, ELCA
- Marco Demarmels, Lake Griffin
- Tony Schaller, medshare

Die Inhalte wurden iterativ erarbeitet und zu den folgenden Terminen mit dem Koordinationsorgan abgestimmt:

28.01.2010	Projektvorbesprechung
1.02.2010	Gemeinsames Kickoff / Abstimmung mit allen Mandaten
17.02.2010	Validierung Fragestellung und mögliche Lösungsansätze
4.03.2010	Validierung Gesamtbild, erste Ausgestaltung und Reifegradmodell Interoperabilität
23.03.2010	Validierung Konkretisierung Gesamtbild, Ausformulierung Use cases, Diskussion von Varianten/Empfehlungen
31.03.2010	Validierung Entwurf mit allen Inhalten
9.04.2010	Ablieferung Schlussbericht

1.4 Struktur dieses Dokumentes

Im Anschluss an die Einleitung (dieses Kapitel) folgt zuerst eine Beschreibung des **„Gesamtbildes der Architektur“ (Kapitel 2)**, welche einerseits einen Gesamtüberblick über die Ausgestaltung gibt, andererseits wichtige Elemente darin definiert und damit einen Orientierungsrahmen für das gesamte weitere Dokument zur Verfügung stellt – inklusive des wichtigen Hilfsmittels **„Reifegradmodell Interoperabilität“ (Kap. 2.5)**.

Die **„Validierung der Ausgestaltung anhand der Use cases“ (Kapitel 3)** demonstriert, wie die Elemente der Architektur die übergreifende Interoperabilität ermöglichen.

Anschliessend folgen in weiteren Kapiteln die Ausgestaltungen der einzelnen Basiskomponenten im Detail.

- Kap. 4: „IT-Infrastruktur (inkl. Anbindung und Austausch)“
- Kap. 5: „Berechtigungssystem“
- Kap. 6: „Patientenindex“
- Kap. 7: „Index Behandelnde“
- Kap. 8: „Dokumentenregister“
- Kap. 9: „Dokumentenablage“
- Kap. 10: „Zugang“

Ein separater Anhang (Kap. 11) führt die referenzierten Dokumente auf und enthält ein Glossar.

2 Gesamtbild der Architektur

Dieses Kapitel definiert das Gesamtbild für die Architektur.

- Kap. 2.1 zeigt eine Übersicht und stellt das Gesamtbild vor (Abbildung 2).
- Kap. 2.2 beschreibt Elemente auf nationaler Ebene und
- Kap. 2.3 die Elemente pro Community.
- Kap. 2.4 definiert Anforderungen an die OID-Registrierung.
- Kap. 2.5 stellt das Reifegradmodell Interoperabilität vor.

Für ein Glossar mit Definition der wichtigsten Begriffe wird in den Anhang in Kapitel 11.2 verwiesen.

2.1 Übersicht

Abbildung 2 zeigt das Gesamtbild und wichtige Elemente des Systems[2] „eHealth Schweiz“. Im Folgenden eine Beschreibung der Grundidee.

Das Gesamtsystem besteht aus einer Menge von **Gemeinschaften / Communities**, welche miteinander interoperabel sind.

- „Gemeinschaft/Community“ ist generisch zu sehen als Gruppe von Organisationen/Systemen, welche im Gesundheitsbereich tätig sind und auf Grund gewisser Gemeinsamkeiten (örtlich / inhaltlich / rechtlich) zusammenarbeiten.
- Eine Community könnte z.B. ein Kanton, ein Spitalverbund oder ein Ärztenetz sein.
- Ein privater Anbieter, welcher ein Patientenportal zur Verfügung stellt, wäre ebenfalls eine Community.
- Ebenso die Anbindung an die europäische eHealth-Infrastruktur für den Austausch von Notfalldaten: der sog. National Contact Point, wie er im Kontext von epSOS[3] nötig sein wird.

Warum „Gemeinschaften / Communities“ und nicht „Domains“?

„Domains“ haben durchaus ähnlich Eigenschaften wie „Communities“. In der Tat könnte eine „Community“ sogar durch eine einzige „Affinity Domain“ realisiert werden[4].

Der Begriff „Domains“ wird in IHE jedoch häufig im Kontext gemeinsamer Infrastrukturen von Repositories und einer Registry gesehen (XDS Affinity Domain). Der Begriff „Community“ wird durch IHE etwas weiter gefasst und kann auch verwendet werden, wenn die interne „Sharing Structure“ nicht auf XDS basiert.

Vgl. Definitionen im Glossar

„Gemeinschaft“ oder „Community“?

- Prinzipiell meinen die beiden Begriffe das gleiche.
- „Community“ entspricht der im Kontext von IHE üblichen Bezeichnung
- „Gemeinschaft“ ist einfach die deutschsprachige Entsprechung.
- Der vorliegende Bericht verwendet daher die folgende Konvention:
  - In Kap. 2 ist stets von „Gemeinschaften/Communities“ die Rede.
  - Ab Kap. 3 wird nur noch IHE-konform der Begriff „Communities“ verwendet.

Die Gemeinschaften/Communities sind mittels **Gateways („Eingangspforten“ / „Netzübergängen“)** miteinander verbunden, welche die übergreifende Zusammenarbeit ermöglichen:

- „Gateway“ ist dabei – analog zu „Communities“ – in einem generischen Sinne zusehen.

[2] System ist an dieser Stelle im Sinne der Systemtheorie als Gesamtheit von Elementen, welche miteinander wechselwirken und in einem bestimmten Kontext stehen, zu verstehen.

[3] epSOS ist ein europäisches eHealth-Projekt, welches in einem ersten Schritt auf „Patient Summary“ / Notfalldaten fokussiert. Siehe http://www.epsos.eu/

[4] Wenn intern IHE XDS zum Einsatz kommt.

- Typischerweise dürfte es sich um ein Anwendungssystem handeln (Hard- und Software, angemessen angebunden an die lokale bzw. übergreifende Netzwerkinfrastruktur).
- Die Anforderungen an die Gateways werden – neben Anforderungen an die interne Ausgestaltung der Communities – ein zentrales Ergebnis der Konkretisierung der Basiskomponenten sein.

Wichtige Eigenschaften der **Topologie** des Gesamtsystems sind:
- Einzelne Organisationen / Beteiligte können in mehreren Communities sein (z.B. im Fall eines Belegarztes, der neben seiner Tätigkeit in der Klinik noch in einer Praxis tätig ist.).
- Eine Community kann mehrere Gateways haben (z.B. wenn ein privater Anbieter weiter gehende Vernetzung anbietet, die über die „Standardfunktionalität" hinausgeht).

2.2 Elemente auf nationaler Ebene

Auf nationaler Ebene gibt es:
- Ein Ensemble von **„Communities"** (→ die hellblau hinterlegten Ellipsen in Abbildung 2)
- Eine **IT-Infrastruktur**, welche die Communities verbindet
  → die Direktverbindungen / der Backbone in Abbildung 2
  Details siehe Kapitel 4.
- Mögliche weiter gehende Funktionalität / Applikationen als Teil der IT-Infrastruktur
  Siehe Diskussion in Kap. 4.2.

Communities können sein:
- Communities, welche praktisch sämtliche Elemente enthalten (Patientenindex, Dokumentregister, Dokumentenablagen, evtl. einen lokalen Behandelndenindex/HPI
  → kantonale Gesundheitsnetzwerke, Spitäler etc.
  → Community B in Abbildung 2
- Communities, welche einen bereichsspezifischen / „sektoriellen[5]" HPI enthalten
  → Community D in Abbildung 2
- Eine spezielle Community, welche den zentralen HPI-Dienst / den Behandelndenverzeichnis-Dienst enthält.
  → Community H in Abbildung 2
- Eine Community, welche dem national übergeordneten Austausch dient (National Contact Point gemäss epSOS)
  → Community N in Abbildung 2
- Communities, welche nur dem Zugang dienen und (mit Ausnahmen) keine eigenen Dokumente führen
  → private Anbieter von ePatientendossier bzw. Versicherungen
  → Community Z in Abbildung 2
  Details siehe Kapitel 10.

Design-Prinzipien:
- Der Anschluss von Communities an das „Gesamtsystem" erfolgt ausschliesslich[6] über die „Gateways" der einzelnen Communities (siehe Kap. 2.3.1).
- Die Gateways der Communities sind über die IT-Infrastruktur verbunden (*Kapitel 4*)
- Einzelne Organisationen können in mehreren Communities sein (z.B. eine Privatklinik in einer „kantonalen Community" wie auch in einem „Klinikverbund").
- Eine Community kann mehrere Gateways haben (z.B. wenn ein privater Anbieter weiter gehende Vernetzung anbietet, die über die „Standardfunktionalität" hinausgeht).

[5] Zum Begriff „sektoriell" vgl. Glossar
[6] Andere Wege sind technisch denkbar, würden dann aber nicht unter die Governance von eHealth Schweiz fallen.

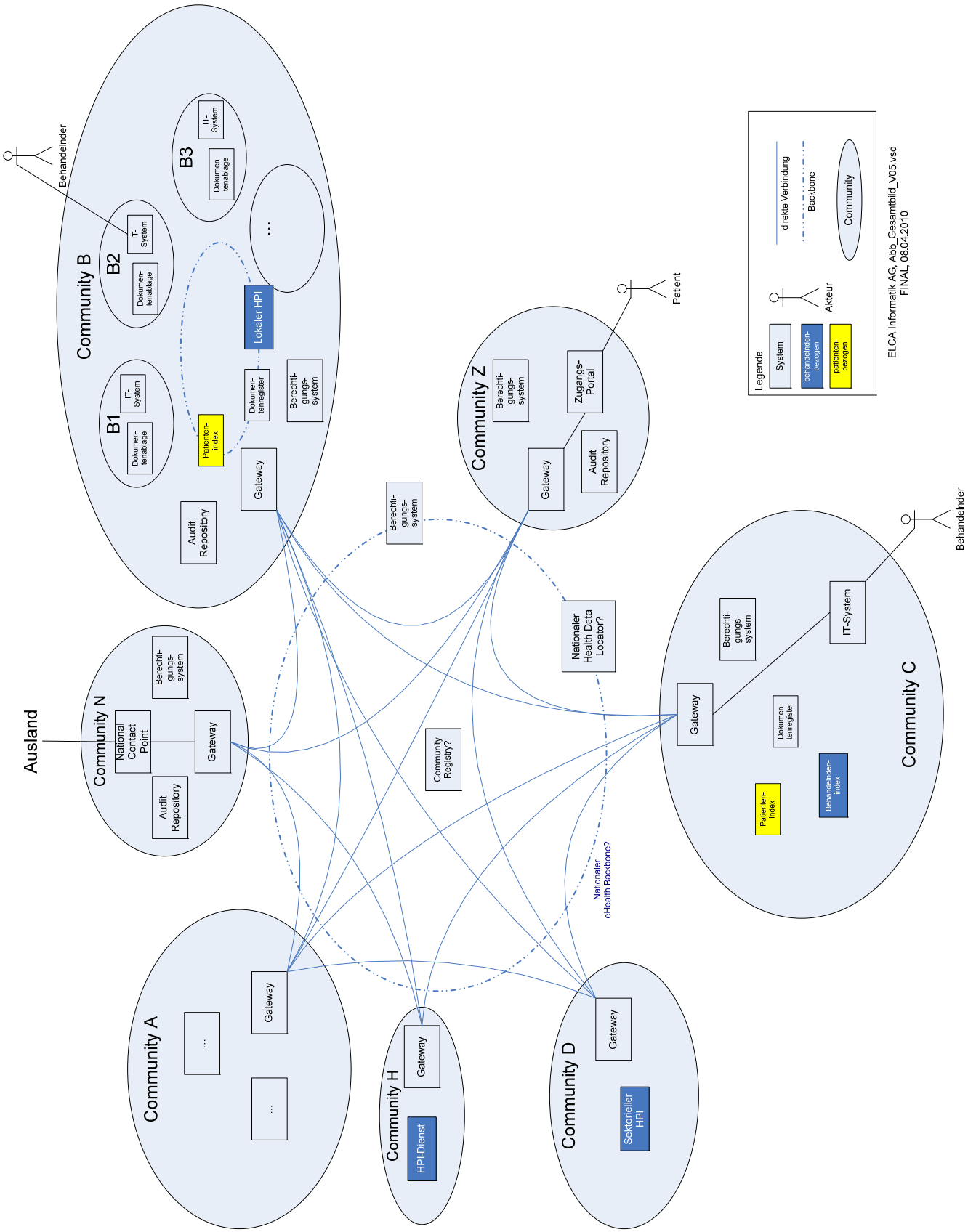


Abbildung 2: Gesamtbild und wichtige Elemente der Architektur (high-level / exemplarisch)

2.2.1 IT-Infrastruktur

Die IT-Infrastruktur ermöglicht das Zusammenspiel / die Interoperabilität der Elemente in den Communities.

Aufgaben:
- Sichere Anbindung der Communities (via Gateways)
- Weiterleiten von Nachrichten von Gateway zu Gateway
- Sicherstellen der Verschlüsselung der Nachrichtenübertragung (Transport Layer Security/TLS)
- *Es gibt verschiedene erweiterte Elemente und Aufgaben, welche Teil der Infrastruktur sein könnten → siehe hierzu Tabelle 4 auf Seite 37*

Design-Prinzipien:
- Die Ausgestaltung der IT-Infrastruktur kann auf einer Community Registry oder einem Backbone basieren
  Für die Variantendiskussion siehe Tabelle 3 auf Seite 35
- Verschlüsselte Nachrichtenübertragung via IHE Profil „Audit Trail and Node Authentication“ (ATNA)
- Gateways müssen Secure Nodes sein.

Weitere Ausgestaltung und Details siehe Kap. 4.

2.2.2 Behandelndenverzeichnisdienst / „HPI-Dienst“

Ein zentraler Verzeichnisdienst, der auf Anfrage durch berechtigte Systeme für Behandelnde, welche am System eHealth Schweiz teilnehmen, gewisse definierte vertrauenswürdige Attribute/Merkmale bereitstellt. Er ist Quelle für beglaubigte Merkmale (Attribute), welche einen Behandelnden beschreiben, dient aber nicht der Authentifizierung des Behandelnden.

Aufgaben:
- Der HPI-Dienst ist ein Verzeichnisdienst, der für Behandelnde, welche am System eHealth Schweiz teilnehmen, gewisse definierte Attribute/Merkmale führt und bereitstellt.
- Behandelnde sollen sowohl anhand ihrer Merkmale gesucht werden können (interaktive Nutzung) wie auch durch automatisierte Abfragen im Kontext von E-Health-Prozesse (transaktionelle Nutzung)
- Die Attribute/Merkmale umfassen
  - Demographische Angaben (z.B. Name, Adresse etc.)
  - Personenidentifikatoren (z.B. GLN)
  - Offizielle Bestätigungen für qualifizierte Ausbildungen
  - Zuordnung von Behandelnden zu Rollen (gemäss Rollenkonzept)
  - Weitere Merkmale wie Zugehörigkeit zu bestimmten Gesundheitsinstitutionen sind möglich
- Der HPI-Dienst dient nicht zur Authentisierung eines Behandelnden, sondern zur Bestätigung von Behauptungen / „Claims“ über einen bestimmten Behandelnden.
  - In der Terminologie des Identity und Access Managements[7] bildet eine solche Auskunft eines HPI-Dienstes einen sogenannten „Claim“, also eine Behauptung über einen Behandelnden.
  - Ein Verzeichnis, welches solche Claims vorhält, wird „Claim Provider“ genannt.
- Führen eines Verzeichnisses von Gesundheitsinstitutionen.
- Zuordnung von Behandelnden zu Institutionen inkl. deren Funktion in der Institution (noch im Detail zu definieren/entscheiden)

[7] Vgl. Glossar

Design-Prinzipien:

- Der HPI-Dienst stellt einen zentralen Zugangspunkt für Informationen in weiteren, dezentralen Quellen dar.
- Historisierung aller Einträge (alle Einträge inkl. ihrer Gültigkeitsdauer werden behalten)
- Ein HPI-Dienst muss vertrauenswürdige Information bereitstellen, so dass eine Anfrage über einen Behandelnden zu einer vertrauenswürdigen Antwort führt.
- Dementsprechend ist der Registrierungsprozess, durch welchen Einträge in datenliefernden HPI erstellt werden, genau mit den zuständigen Organisationen geregelt.
- Positionierung innerhalb des Gesamtbildes
  - Im System eHealth Schweiz gibt es genau einen HPI-Dienst mit dieser Funktion *Lokale/sektorielle HPI, welche die führenden Systeme für diese Behandelndeninformationen sind, kann es beliebig viele geben.*
  - Der zentrale HPI-Dienst kann in einer eigenen dedizierten Community sein. Er kann jedoch auch Teil einer Community mit weiteren Funktionen sein. In jedem Fall wird er über einen Gateway an das Gesamtsystem angeschlossen.

Weitere Ausgestaltung und Details siehe Kap. 7.

2.2.3 National Contact Point (NCP)

Der National Contact Point ist eine spezielle Community, welche den eigentlichen NCP gemäss epSOS enthält und so die Schweiz an die europäische (epSOS-)Infrastruktur anbindet.

Aufgaben:

- Bidirektionale Anbindung des Systems „eHealth Schweiz“ an die europäische (epSOS-) Infrastruktur
- Nach Bedarf semantisches Mapping
- Sicherstellung von Trust, Vertraulichkeit und Datenschutz mit NCP anderer Länder

Design-Prinzipien:

- Eigentlicher NCP gemäss Vorgaben epSOS
- Anbindung an die weiteren Communities über einen Gateway wie die anderen Communities (siehe Kap. 2.3.1). Damit kann auch ein Mapping von Rollen umgesetzt werden.

Abgrenzung / offener Teilbereich:
Auf Grund fehlender übergeordneter Ausgestaltung klammert der vorliegende Bericht den über epSOS hinaus gehenden Datenaustausch mit dem Ausland aus.
(Ausnahme: „Use case 7: „Zugriff auf verteilte med. Daten über Landesgrenzen hinweg“ in Kap. 3.2 zeigt relativ high-level einen möglichen Ablauf für einen derartigen Datenaustausch.)

In allgemeiner Form ist diese Thematik zu klären, falls es entsprechende übergeordnete Ausgestaltungen gibt.

2.2.4 Health Data Locator (evtl.)

Der Health Data Locator führt eine Liste von Communities, in welcher für einen Patienten Daten vorhanden sind, und fördert so die Performance des Gesamtsystems.

Siehe auch die entsprechende Diskussionen in Tabelle 4 auf Seite 35 bzw. die Variantendiskussion in Tabelle 5 auf Seite 38.

2.2.5 Ein nationales Berechtigungssystem (evtl.)

Das nationale Berechtigungssystem verwaltet – falls nötig – Berechtigungen, welche auf nationaler Ebene geführt werden müssen.

Weitere Ausgestaltung und Details zum Berechtigungssystem allgemein siehe Kap. 5.

2.3 Elemente pro Community

Damit das Gesamtsystem „eHealth Schweiz“ ein funktionierendes Ganzes bildet, muss es pro Community gewisse Elemente geben, welche zwingend nötig sind – sei es als einzelne konkrete Systeme oder in einem hierarchischen / lokalen Verbund mehrerer Systeme:

- Kap. 2.3.1: Community Gateway
- Kap. 2.3.2: Audit-Repository
- Kap. 2.3.3: Patientenindex
- Kap. 2.3.4: Community-spezifische HPI („Sektorielle“ bzw. „lokale“ HPI)
- Kap. 2.3.5: Dokumentenregister
- Kap. 2.3.6: Lokale Dokumentenablagen

Diese Elemente werden in den folgenden Unterkapiteln definiert und kurz beschrieben.

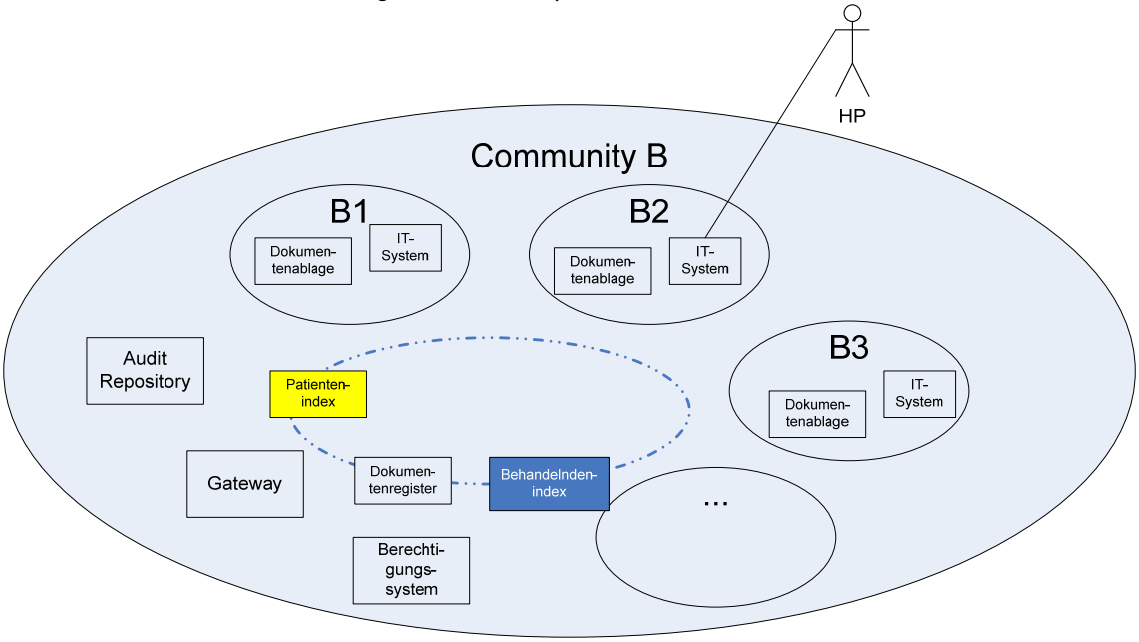


Abbildung 3: Illustration der community-spezifischen Element (Ausschnitt aus Abbildung 2)

Die folgenden Unterkapitel beschreiben die einzelnen Elemente.

2.3.1 Community Gateway

Der Gateway der Community ermöglicht die Interoperabilität der Systeme in der Community mit Systemen in anderen Communities innerhalb des Systems eHealth Schweiz. Er vereint verschiedene Gateways für spezifische Funktionalität wie in folgender Abbildung illustriert.

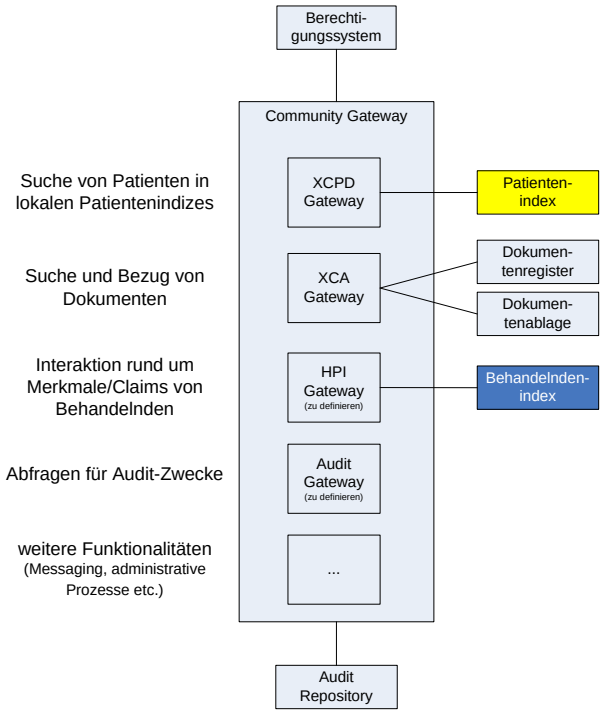


Abbildung 4: Die Community Gateways bestehen aus verschiedenen Applikationen mit dedizierten Aufgaben, welche mit den Systemen in der Community interagieren und deren Interoperabilität im Gesamtsystem eHealth Schweiz sicherstellen.

Aufgaben:

- Weiterleiten von Anfragen von aussen nach innen
- Weiterleiten von Anfragen von innen nach aussen
- Suchen von Patienten mittels demographischer Daten / mittels Patienten-ID
- Suche von Dokumenten für einen bestimmten Patienten / für eine gegebene Dokumenten-ID
- Abholen und Weiterleiten von Dokumenten
- Berücksichtigung der definierten Berechtigungen
- Logging sämtlicher Aktivitäten und Bereitstellung für Audit-Zwecke

Design-Prinzipien:

- Bei sämtlichen Aktivitäten werden die definierten Berechtigungen berücksichtigt (speziell der jeweils definierte Patient Consent).
- Für Dokumentensuche und -abholen kommen zur Anwendung:
  - Zwischen den Gateways: IHE XCA
  - Innerhalb der Communities:
    falls weitere „Unter“-Communities vorhanden: empfohlen IHE XCA
    falls nur eine XDS Affinity Domain: direkt über IHE XDS
- Für Patientensuche kommen zur Anwendung
  - Zwischen den Gateways: IHE XCPD
  - Innerhalb der Communities: IHE PIX/PDQ empfohlen
- Information Hiding: Daten die nicht über die Schnittstelle ausgetauscht werden, sind der anderen Community verborgen

- Entkopplung: Eine Community kann sich intern reorganisieren, ohne dass eine andere Community betroffen ist.

2.3.2 Audit-Repository

Das Audit-Repository stellt sicher, dass sämtliche Aktivitäten nachverfolgbar sind und die Anforderungen des Datenschutzes erfüllt werden.

Aufgaben:
- Protokollierung sämtlicher sicherheitsrelevanter Aktivitäten. Das Audit Log zeichnet Datenzugriffe durch Benutzer und Systeme auf
- Bereitstellung der Protokollierung für Audit-Aktivitäten
- Unterstützung/Logging von Security Policies
- Das Community Gateway protokolliert sämtliche sicherheitsrelevante Aktivitäten direkt im Audit-Repository (vgl. Abbildung 4)

Design-Prinzipien:
- Jede Transaktion (XDS, XCA, mögliche weitere) ist sicherheitsrelevant und muss dementsprechend geloggt werden.
- Grundsätzliche Elemente des Loggings via IHE ATNA

2.3.3 Patientenindex

Der Patientenindex stellt ein Verzeichnis der Patienten in der Community zur Verfügung.

Aufgabe
- Patient registrieren und unter einer lokalen Patienten-ID ablegen
- Administrative Patientendaten / demografische Daten historisiert verwalten
- Patient suchen anhand demografischer Daten / Merkmale oder lokaler Patienten-ID

Designprinzipien
- Eine Patienten-ID ist einer Person in einem bestimmten Bereich dauerhaft eindeutig zugeordnet.
- Eine Patienten-ID wird durch eine Assigning Authority zugeteilt.
- Jede Assigning Authority hat eine weltweit eindeutige ID (z.B. eine OID wie bei IHE-Actor Patient Identity Source).
- Zur eindeutigen Identifikation eines Patienten muss die Patienten-ID und die ID der entsprechenden Assigning Authority angegeben werden.
- Patientendaten sollten von hoher Datenqualität sein und möglichst Merkmale für ein sicheres Matching enthalten (siehe Diskussion unten).
- Einer Person können lokal auch mehrere Patienten-IDs zugeordnet sein (z.B. falls der Patient nicht identifiziert werden konnte, als die Daten angelegt wurden).
- Patientendaten werden lokal verwaltet.
- In einer Community kann es mehrere Patientenindizes geben.
- In einer Community können mehrere Assigning Authorities (Patientenidentifikationsdomänen) benutzt werden.
- In einer Community kann es einen Master Patient Index (MPI) geben.
- Die Patientenindizes sind an den Community Gateway angebunden und sind so vom Gesamtsystem eHealth Schweiz abfragbar.

Weitere Ausgestaltung und Details siehe Kap. 6.

2.3.4 Community-spezifische HPI („Sektorielle“ bzw. „lokale“ HPI)

„Sektorielle HPI“ sind dezentrale Verzeichnisse (z.B. von Berufsverbänden), welche die vertrauenswürdigen Personendaten halten, welche durch den zentralen HPI-Dienst abfragbar sind.

Aufgaben:
- Halten und Pflegen der autoritativen Personendaten
- Bereitstellung dieser Daten an den HPI Schweiz

Design-Prinzipien:
- Die Bereitstellung der Daten der sektoriellen HPI an den HPI Schweiz erfolgt je nach Variante durch Datenlieferungen oder als Abfragemöglichkeiten
- Gewisse Aspekte sind auszugestalten gemäss übergeordneten Richtlinien im Sinne des Systems eHealth Schweiz

„Lokale HPI“ sind typischerweise Teil des lokalen Identity and Access Managements (IAM) und verwalten spezifische / lokale Attribute/Merkmale von Behandelnden.

Aufgaben:
- Verwalten von spezifischen / lokalen Attribute/Merkmale von Behandelnden.
- Bereitstellung dieser Daten für das lokale IAM-System

Design-Prinzipien:
- Ausgestaltung nach lokalen Anforderungen
- Typischerweise nicht mit HPI Schweiz integriert (vermutlich bis auf Verwendung gewisser gemeinsamer Attribute/Merkmale)

Weitere Ausgestaltung und Details siehe Kap. 7.

2.3.5 Dokumentenregister

Das Dokumentenregister (Document Registry) der Community stellt sicher, dass die Dokumententypen und Dokumente recherchierbar sind.

Aufgaben:
- Registrierung von Dokumenten mit Metadaten
- Ermöglichen der Suche von Dokumenten anhand der Metadaten
- Ermöglichen der Suche von Dokumenten mittels Dokument-ID

Design-Prinzipien:
- In den Metadaten eines Dokuments werden lokale Patienten-ID, Dokumenten-ID, Repository-ID und Behandelnden-ID verknüpft.
- Ein Dokumentenregister wird durch den Aktor „Document Registry“ des IHE-Profils XDS.b realisiert.
- Für eine XDS Affinity Domain sollte definiert werden, welche Dokumenttypen, -formate und XDS-Metadaten zugelassen sind.
- Auf das Dokumentregister greifen direkt nur Systeme der Community zu. Mittels Gateways ist auch ein Zugriff von anderen Communities aus möglich. Ein XCA-Gateway stellt die Schnittstelle für den Zugriff bereit.
- Der Zugriff auf die Document Registry wird über das Berechtigungssystem kontrolliert und protokolliert.

Weitere Ausgestaltung und Details siehe Kap. 8.

2.3.6 Lokale Dokumentenablagen

Ein oder mehrere lokale Dokumentenablagen (Document Repositories) dienen der strukturierten Ablage von Dokumenten.

Aufgaben:
- Dokumente können mit einer ID gespeichert werden.
- Dokumente können mit einer ID abgeholt werden.
- Die Integrität der Daten wird sichergestellt.

Design-Prinzipien:
- Die Dokumentenablagen müssen an einen XCA-Gateway angebunden werden können.
- Die Dokumenten-ID ist weltweit für immer eindeutig und an einen festen Dokumentinhalt gekoppelt.
- Der Inhalt des Dokuments spielt eigentlich keine Rolle. Dokumente werden genauso zurückgegeben, wie sie abgelegt wurden. (Inhalte, Signatur, Verschlüsselung etc. müssen woanders definiert werden – Richtlinien)

Weitere Ausgestaltung und Details siehe Kap. 9.

2.4 Anforderungen an die OID-Registrierung

Nachfolgende Kandidaten für OIDs wurden gemeinsam mit dem Rollenkonzept erarbeitet. Die Liste hat keinen Anspruch auf Vollständigkeit und die Nennungen sind als erste Überlegungen zu verstehen. In jedem Fall müssen die, zu registrierenden OIDs bei Umsetzung genau geprüft werden. Dabei sind die, im [OID Konzept] genannten Grundsätze und Regeln anzuwenden.

Anregung für die weitere Umsetzung: Für die Identifikation von Personen und Institutionen bräuchte es eigentlich nur SuisseID (für Personen) und UID (für Unternehmen und Institutionen), sowie die Zuordnung zwischen SuisseID und UID für Arbeitnehmerverhältnisse. Diese Elemente können sowohl für Behandelnde wie auch für Patienten genutzt werden. Bei der Umsetzung muss diesbezüglich allerdings eine wichtige Frage geklärt werden: „Wer ist Claim-Provider für Arbeitnehmerverhältnisse“?

Für folgende **Identifikationen** (resp. den entsprechenden Domänen) sind OIDs notwendig:
- Gateways resp. Community Identifikatoren (inkl. NCP; XDS Affinity Domains)
- MPIs, sowie lokale Patienten IDs, sofern diese community-übergreifend im Einsatz sind
- HPIs, (zentraler Verzeichnisdienst, sektorielle HPIs und Lokale HPIs sofern diese community-übergreifend im Einsatz sind). Bei Unterteilung analog zu Australien auch HPI-I und HPI-O
- Dokumentenregister inkl. allenfalls Health Data Locator (weltweit eindeutige Dokumenten IDs)
- Dokumentenablagen (weltweit eindeutige Dokumenten IDs)
- Autorisierungskennungen von Patienten für die Anmeldung am Patientendossier
- Kryptografische Ableitung der neuen AHV Nummer
- MedReg
- Versichertenkarte
- Health Professional Card (HPC)
- SuisseID
- Unternehmensidentifikationen (UID)
- Audit Repositories
- Patient Consents
- Claim Provider
- Patientendossiers (Portale/Sekundärsysteme mit Verwaltung durch Patient)

- Erbringungsorte (physikalische Lokation) für Bezug zwischen Behandelnden und Standorten/Adressen (im Hinblick auf Berechtigungskonzept: Zuordnung von Behandelnden zu Institutionen inkl. deren Funktion in der Institution)
- DAC[8] Listen (z.B. Blacklists / Whitelists)

Allenfalls weitere (ergibt sich bei Umsetzung):
- gemäss IHE Profilvorgaben
- gemäss noch zu erarbeitendem Berechtigungskonzept

Hinweise: Für folgende Elemente bestehen bereits OIDs (siehe www.hl7.ch/oid):
- AHV alt: 2.16.756.5.31 (NAVS11)
- AHV neu: 2.16.756.5.32 (NAVS12)
- GS1 GLN (EAN): 1.3.88 (vgl. CDA-CH)
  (ist eine weitere Möglichkeit neben den oben genannten SuisseID und UID

Für folgende **Codesysteme** sind entsprechende OIDs notwendig:
- Berufsgruppen (strukturelle Rollen; eigenes oder SNOMED-CT)
- Rollen (funktionale Rollen)
- Sensitivitätslevels (z.B. ConfidentialityCode Standard aus HL7, Erweiterung gemäss IHE BPPC)
- Dokumentkategorien (z.B. CEN13606 + HUG), Dokumentenarten (OID für MIME Type?)
- Erbringungsorte (Kategorisierung physischer Erbringungsorte; Bezug zu Abteilung (z.B. Chirurgie, Physiotherapie); im Hinblick auf Berechtigungskonzept)
- Medizinischer Kontext (im Hinblick auf Berechtigungskonzept; eigenes oder SNOMED-CT)
- HPI Weiterbildungstitel
- Falls Klassifikation der Health Professionals gemäss Kapitel 7.1.4 gewünscht ist auch:
  - Provider Individual Type (Weiterbildungstitel)
  - Provider Individual Speciality (Subspezialität)
  - Provider Individual Specialisation (Subsubspezialität)
- ATNA Log Kategorien (Inhalt eines Log-Eintrags gemäss RFC 3881):
  - Event Identification (Was ist geschehen?)
  - Active Participant Identification (Durch wen ?)
  - Network Access Point Identification (Wo?)
  - Audit Source Identification (Womit?)
  - Participant Object Identification (Auf welchen Datensatz?)
  - [Erweiterungen möglich]
- epSOS Kategorien für Austausch über NCP
- Tarife (Tarmed, kantonale Tarife)
- Diagnosen (z.B. TI-Code, ICPC-2, ICD10-CH, ICD9-cm/CHOP Code)
- SwissDRG

[8] Discretionary Access Control

2.5 Reifegradmodell Interoperabilität

Dieses Unterkapitel definiert ein Reifegradmodell Interoperabilität für die Architektur bzw. die einzelnen Komponenten. Ziele dieses Modells sind:

- Bereitstellung einer Messlatte in Bezug auf die Konformität und Integrierbarkeit mit der Gesamtarchitektur eHealth Schweiz
  → für Zwischenschritte („auf dem Weg zur Zielarchitektur“)
  → für Mindestanforderungen
- Reduktion der Komplexität und Bereitstellung einer Hilfe für die Entwicklung der Beteiligten und ihrer IT-Systeme
  → Unterstützung bei Entscheidung (z.B. zur Beschaffung / Weiterentwicklung von Systemen)
  → Reduktion von Hürden und Risiken
  → Förderung Investitionssicherheit
- Erhöhung Transparenz / Aufzeigen eines Weges hin zu den hohen Reifegradstufen
  → für einzelne Teilnehmer
  → für das Gesamtbild eHealth Schweiz

Kategorie	Stufe	Charakterisierung
nationale / übergreifende Interoperabilität	A1	• Verwendung von Standards, welche die Interoperabilität über die Schweiz hinaus ermöglichen.
	A2	• Systeme arbeiten „voll interoperabel“ auf nationaler Ebene zusammen; regionale/sektorspezifische Systeme können über entsprechende Profile Informationen austauschen
regionale / sektorspezifische Interoperabilität	B1	• Verwendung von Standards und IDs, welche Basis bilden für eine zukünftige regions-/sektorübergreifende Interoperabilität (z.B. Ausgestaltung eines kantonalen Systems nach übergeordneten Kriterien jedoch noch ohne übergeordnete Integration)
	B2	• Verfügbarkeit regionaler/sektorspezifischer Systeme/Indizes (z.B. MPI SG als regionales Beispiel; MedReg als sektorspezifisches Beispiel)
lokale elektronische Abwicklung	C1	• Verwendung von Standards und IDs, welche Basis bilden können für zukünftige regionale / sektorspezifische Zusammenarbeit
	C2	• lokale, strukturierte Systeme für elektronische Abwicklung existieren (z.B. Datenbanken, DMS)
keine oder nur sehr beschränkte elektronische Abwicklung	D1	• Informationen elektronisch vorhanden, jedoch ohne Sicherstellung konsistenter Strukturen und Konsistenz (z.B. in Form von Excel-Listen, gescannten Dokumenten in einem Verzeichnis)
	D2	• Papierbasierte Ablage und Abwicklung

Tabelle 1: Vorschlag Reifegradstufen Interoperabilität

Anwendung für die Konkretisierung der Basiskomponenten:

- Pro Komponente Beschreibung der Merkmale und Voraussetzungen für die Erreichung der einzelnen Stufen
  → „Prüfkriterien“ / „Indikationen“

Verweise auf weiter gehende Konkretisierungen:
Die folgenden Kapiten enthalten spezifische Anforderungen / Mindestkriterien für die verschiedenen Reifegradstufen:
Kap. 6: Patientenindex
Kap. 7: Index Behandelnde
Kap. 8: Dokumentenregister
Kap. 9: Dokumentenablage

Ergänzende Bemerkungen:

- Die Skala wurde in Anlehnung an das Wirtschaftlichkeitsmodell für E-Government der CSP gewählt [EGov-ModellCSP].
  Andere Skalen (z.B. Energie-Etiketten Fahrzeuge A..G oder analog CMMI/SPICE 0..5) wären analog möglich
  - Die jeweilige x2-Stufe ist die Minimalstufe für die Erreichung der jeweiligen Interoperabilität.
  - Die jeweilige x1-Stufe legt den Grundstein für die darüber liegende Interoperabilität.
- **Gesamtfokus / Ziel ist übergreifende Interoperabilität auf nationaler Ebene (=A2)**
  (mit der geforderten internationalen Integration / epSOS)
  (untere Stufen nur illustrativ / wo sinnvoll im Link nach oben)

2.6 Nächste Schritte / offene Punkte

Titel	**Spezifikation von Richtlinien für Communities (inkl. gesetzl. Grundlagen)**
Details	Richtlinien für die Bildung einer Community (gegebenenfalls aus bestehenden Communities) müssen definiert werden. Für einen domänenübergreifenden Datenaustausch müssen rechtliche Grundlagen geschaffen werden. Eine Community muss bei einem OID-Register registriert werden, um eine weltweit eindeutige ID zu erhalten (homeCommunityId). Richtlinien, wie mit lokalen IDs (z.B. Patienten-IDs, Behandelnden-IDs) in Metadaten umgegangen werden soll

Titel	**Operationalisierung des Reifegradmodells**
Details	Klärung offener Punkt: - Form der Anwendung? - Anwendung auf was genau und in welcher Form? - Sollen die mittleren Reifegradstufe B nur die geographische Hierarchie abbilden oder auch Sektoren? (z.B. die verschiedenen Arten Behandelnder?) - Welche Reifegrade werden im Kontext der Anwendungsfelder / Hierarchien / Sektoren genau bestimmt? (z.B. MedReg könnte als A1 Element gesehen werden oder sektorspezifisches B2 Element) Im Kontext der Operationalisierung zu klären: - Welche Prüfungen müssen wann gemacht werden? - Wer führt Prüfungen genau durch? - Finanzierung der Prüfungen?

3 Validierung der Ausgestaltung anhand der Use cases

Dieses Kapitel dient der Validierung der Ausgestaltung der Basiskomponenten anhand der folgenden Use cases [UseCaseDokument]:

- Use case 5: „Nachvollziehbarkeit
- Use case 7: „Zugriff auf verteilte med. Daten über Landesgrenzen hinweg
- Use case 10 „Notfallbehandlung TI-SG“
- Use case 12 „Behandlungsauthentisierung”

Die Auswahl der Use cases wurde mit dem Koordinationsorgan abgesprochen.

Ziel der folgenden Ablaufdarstellungen ist es, das Funktionieren der Basiskomponenten im Kontext der verschiedenen Fallbeispiele zu illustrieren. Die Nachrichtenprotokolle und die genau ausgetauschten Metadaten waren nicht Teil des Mandats und sind deshalb illustrativer Natur.

Erläuterungen zur Beschreibung der Use case-Abwicklung:

- Die Notation entspricht einer high-level Prozessbeschreibung in BPMN (pragmatisch angewandt).
- Die rechteckigen Kästchen sollen mitgeführte Daten symbolisieren
  - B.M. = Beate Muster
  - 1.1.70 = Geburtstag von B.M. (exemplarisch für demographische Daten)
  - TI4711 = Identifikator im Tessin
  - SG313 = Identifikator in St. Gallen
  - 212, 247, 337 = Dokumenten-IDs
- 

steht für „Security Tokens“ (typischerweise „SAML Assertions“), welche die Authentizität und Integriert der Information sicherstellt.

Zur Genauigkeit / Vollständigkeit:
Die Abläufe sollen das Funktionieren der Basiskomponenten „illustrieren“. Sie stellen also keine 100%ig korrekte und im Detail vollständige Beschreibung der jeweiligen Anwendungsfälle dar.

Siehe auch offenen Punkt / nächsten Schritt in Kap. 3.5.

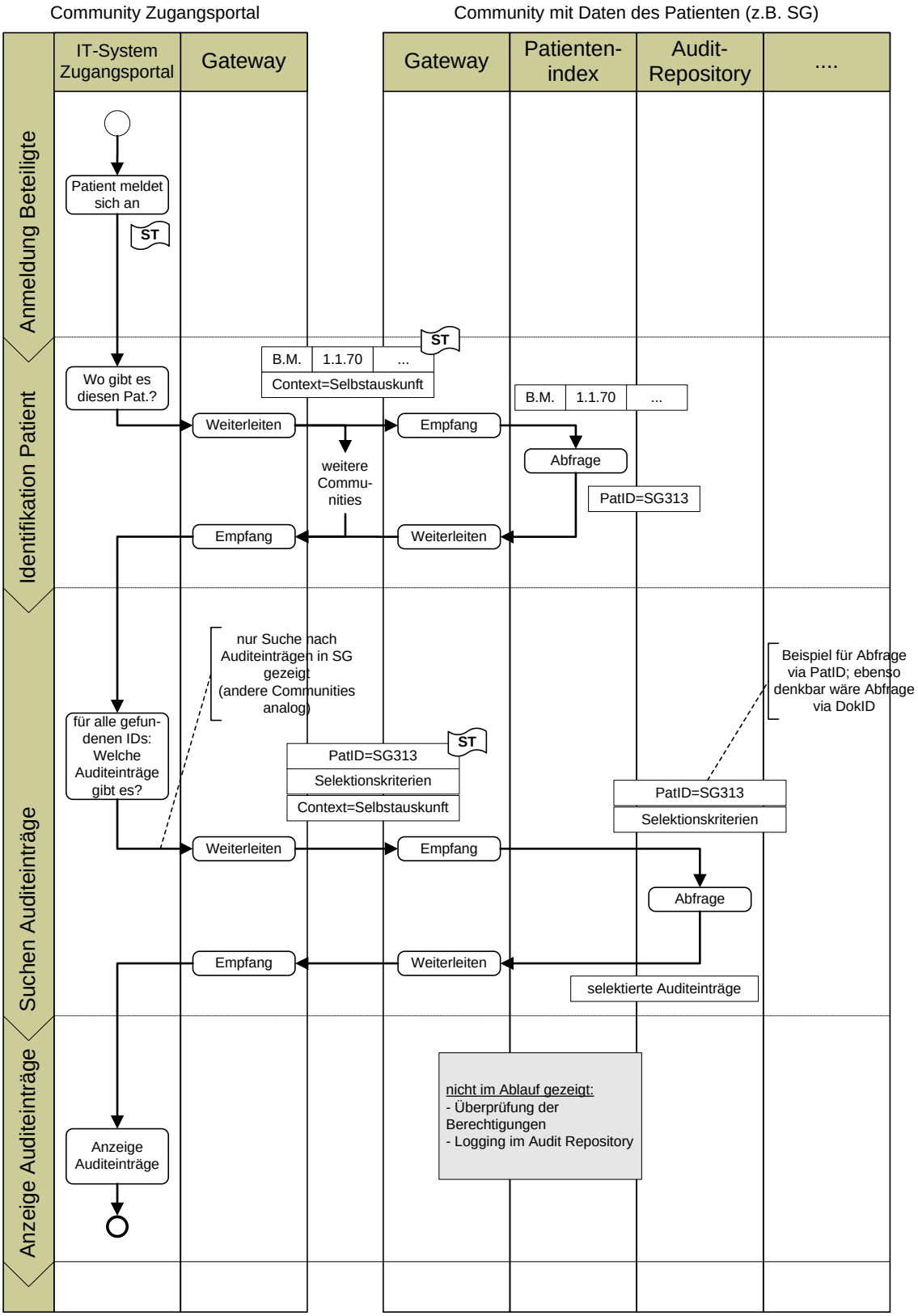
3.1 Use case 5: „Nachvollziehbarkeit“

Beschreibung des Use cases [UseCaseDokument]:

Annahme:
Ein Patient möchte zu einem gewünschten Zeitpunkt (z.B. nach einem Notfall) alle Zugriffe auf sein Patientendossier kontrollieren.

Beschreibung:
Der Patient meldet sich bei dem System (z.B. Zugangsportal) an, das sein Patientendossier bereitstellt. Das System zeigt dem angemeldeten Benutzer alle Zugriffe auf die Daten seines elektronischen Patientendossiers an.

Akteure:
Patient


Community Zugangsportal
Community mit Daten des Patienten (z.B. SG)
IT-System Zugangsportal
Gateway
Gateway
Patienten-index
Audit-Repository
....
Anmeldung Beteiligte
Identifikation Patient
Suchen Auditeinträge
Anzeige Auditeinträge
Patient meldet sich an
ST
Wo gibt es diesen Pat.?
B.M.
1.1.70
...
Context=Selbstauskunft
Weiterleiten
Empfang
weitere Commu-nities
Abfrage
PatID=SG313
Empfang
Weiterleiten
nur Suche nach Auditeinträgen in SG gezeigt (andere Communities analog)
Beispiel für Abfrage via PatID; ebenso denkbar wäre Abfrage via DokID
für alle gefun-denen IDs: Welche Auditeinträge gibt es?
PatID=SG313
Selektionskriterien
Context=Selbstauskunft
Weiterleiten
Empfang
Abfrage
selektierte Auditeinträge
Empfang
Weiterleiten
nicht im Ablauf gezeigt:
- Überprüfung der Berechtigungen
- Logging im Audit Repository
Anzeige Auditeinträge

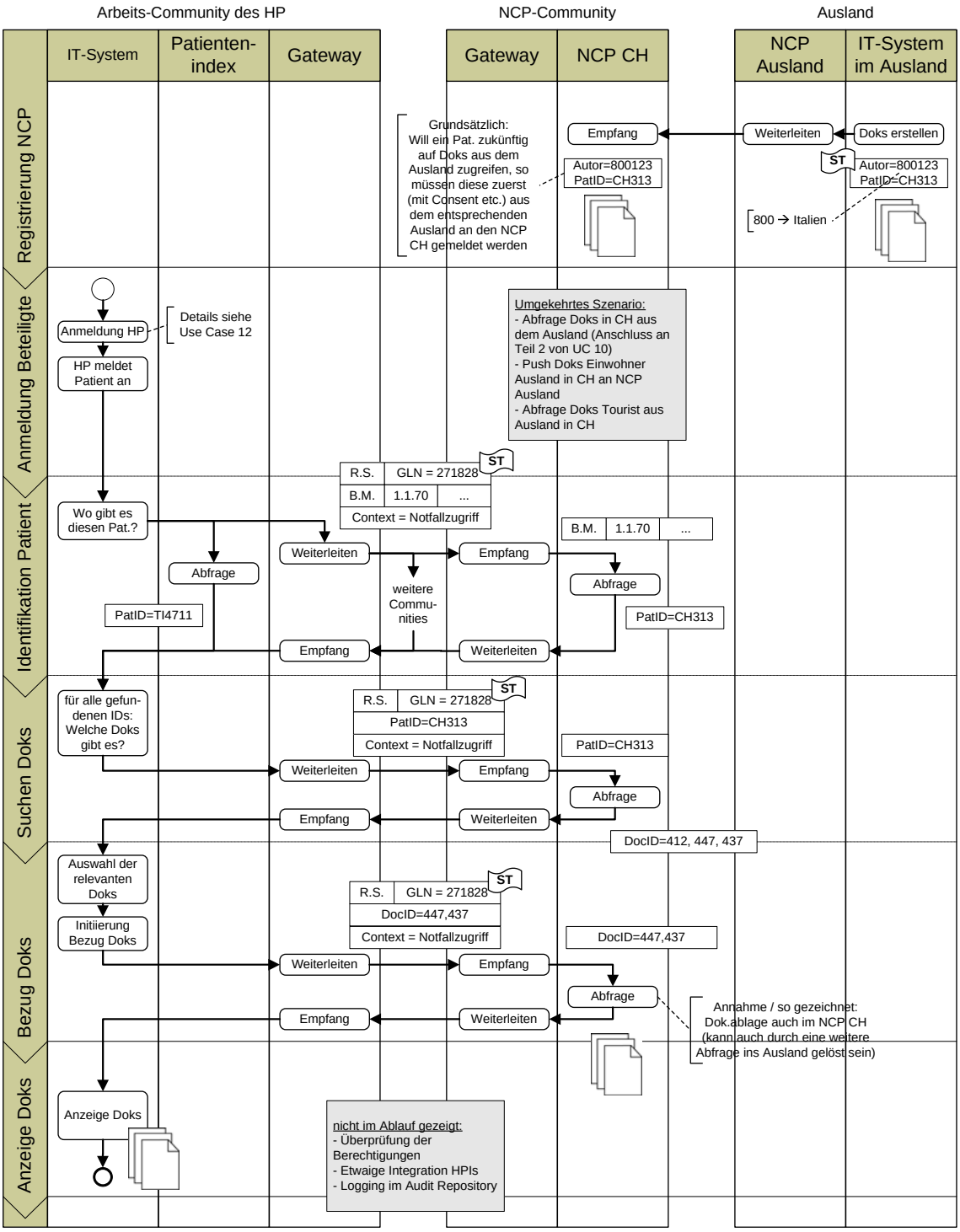
3.2 Use case 7: „Zugriff auf verteilte med. Daten über Landesgrenzen hinweg“

Beschreibung des Use cases [UseCaseDokument]:

Annahmen:
1. Ein Arzt stellt Patientendaten immer nur in seiner Domäne zur Verfügung.
2. Ärzte sollten domänenübergreifend Patientendaten abfragen können, auch wenn eine Domäne im Ausland liegt.
3. Die Domäne ausserhalb der Schweiz muss hierbei nicht zwingend eine IHE-Domäne sein.

Beschreibung:
Der Arzt greift auf die Daten des Patienten in einer Domäne im Ausland zu.

Akteure:
Patient, Arzt in der Schweiz, Arzt im Ausland


Arbeits-Community des HP
NCP-Community
Ausland
IT-System
Patienten-index
Gateway
Gateway
NCP CH
NCP Ausland
IT-System im Ausland
Registrierung NCP
Anmeldung Beteiligte
Identifikation Patient
Suchen Doks
Bezug Doks
Anzeige Doks
Grundsätzlich: Will ein Pat. zukünftig auf Doks aus dem Ausland zugreifen, so müssen diese zuerst (mit Consent etc.) aus dem entsprechenden Ausland an den NCP CH gemeldet werden
Empfang
Weiterleiten
Doks erstellen
ST
Autor=800123
PatID=CH313
800 → Italien
Anmeldung HP
Details siehe Use Case 12
HP meldet Patient an
Umgekehrtes Szenario:
- Abfrage Doks in CH aus dem Ausland (Anschluss an Teil 2 von UC 10)
- Push Doks Einwohner Ausland in CH an NCP Ausland
- Abfrage Doks Tourist aus Ausland in CH
R.S.
GLN = 271828
B.M.
1.1.70
...
Context = Notfallzugriff
Wo gibt es diesen Pat.?
Weiterleiten
Empfang
Abfrage
weitere Commu-nities
PatID=TI4711
PatID=CH313
Empfang
Weiterleiten
für alle gefun-denen IDs: Welche Doks gibt es?
PatID=CH313
DocID=412, 447, 437
Auswahl der relevanten Doks
Initiierung Bezug Doks
DocID=447,437
Annahme / so gezeichnet: Dok.ablage auch im NCP CH (kann auch durch eine weitere Abfrage ins Ausland gelöst sein)
Anzeige Doks
nicht im Ablauf gezeigt:
- Überprüfung der Berechtigungen
- Etwaige Integration HPIs
- Logging im Audit Repository

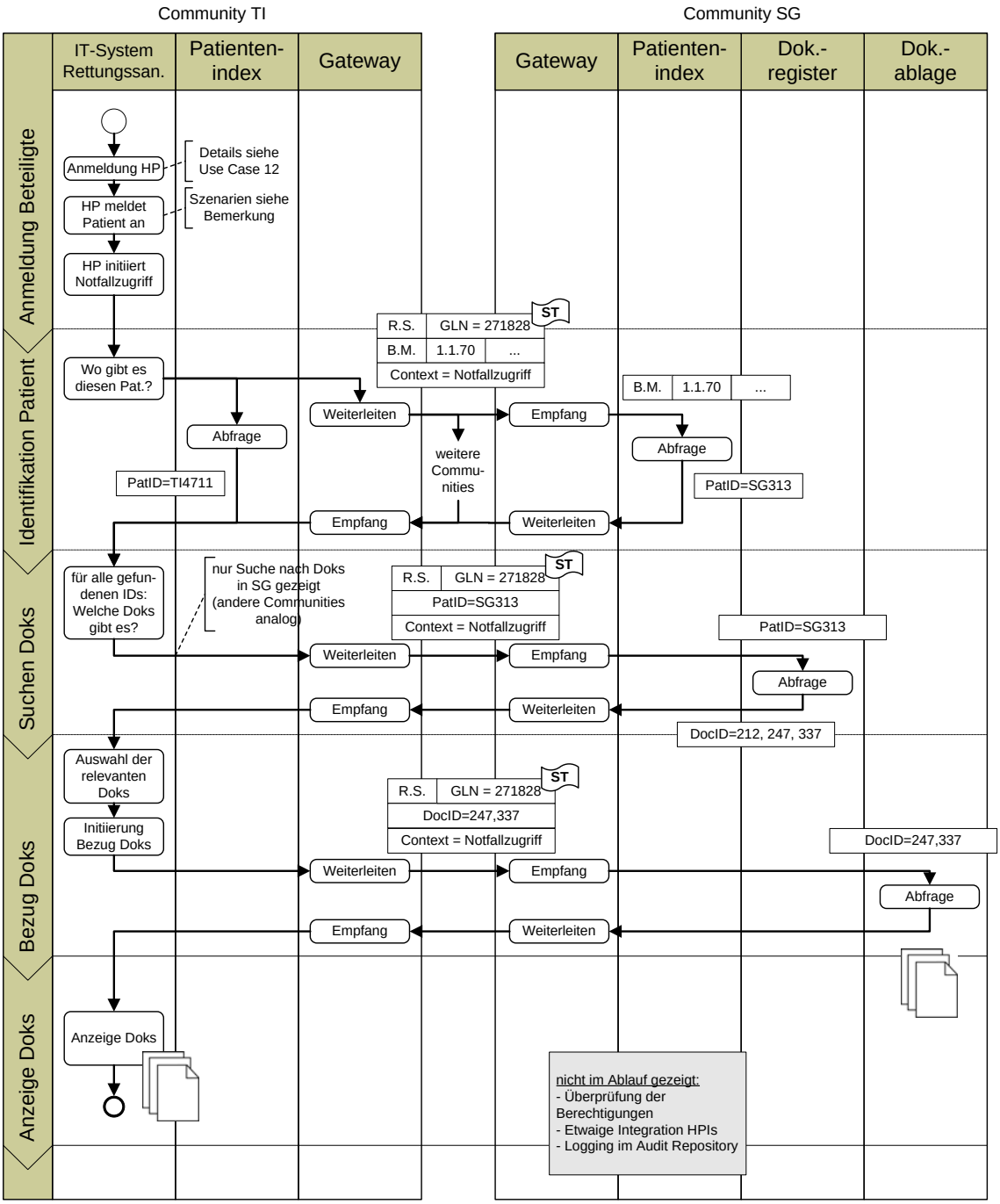
3.3 Use case 10 „Notfallbehandlung TI-SG“

Beschreibung des Use cases [UseCaseDokument]:

Annahme:
Frau Beate Muster aus St. Gallen verunfallt im Kanton Tessin auf der Autobahn und ist bewusstlos. Der Notarzt von Lugano benutzt das ePD des Kantons Tessin welches somit eine eigene Domäne darstellt. Die meisten medizinischen Daten von Fr. Beate Muster sind in der Domäne des Kantons St. Gallen zu finden.

Beschreibung:
Der Notarzt des Tessiner Rettungsdienstes versorgt die bewusstlose Patientin vor Ort auf der Autobahn. Durch die neue Versichertenkarte kann der Rettungssanitäter weitere medizinische Daten der Patientin im Kanton St. Gallen ausfindig machen. Auch ohne die explizite Zustimmung kann der Notarzt oder Rettungssanitäter die Daten einsehen. Es stellt sich heraus, dass sie eine Penicillin-Allergie hat und momentan wegen einer künstlichen Herzklappe ein Blutverdünnungsmittel einnimmt. Diese Information wird an den Schockraum im Spital Lugano weitergegeben. Nach erfolgter Behandlung im Spital Lugano werden die wesentlichen medizinischen Daten in das ePD des Kantons Tessin eingetragen und können nun aus St. Gallen eingesehen werden.

Akteure:
Notarzt, Rettungssanitäter, Spitalarzt, Pflegekräfte im Spital, Hausarzt



(Fortsetzung des Use Case siehe weiter hinten.)

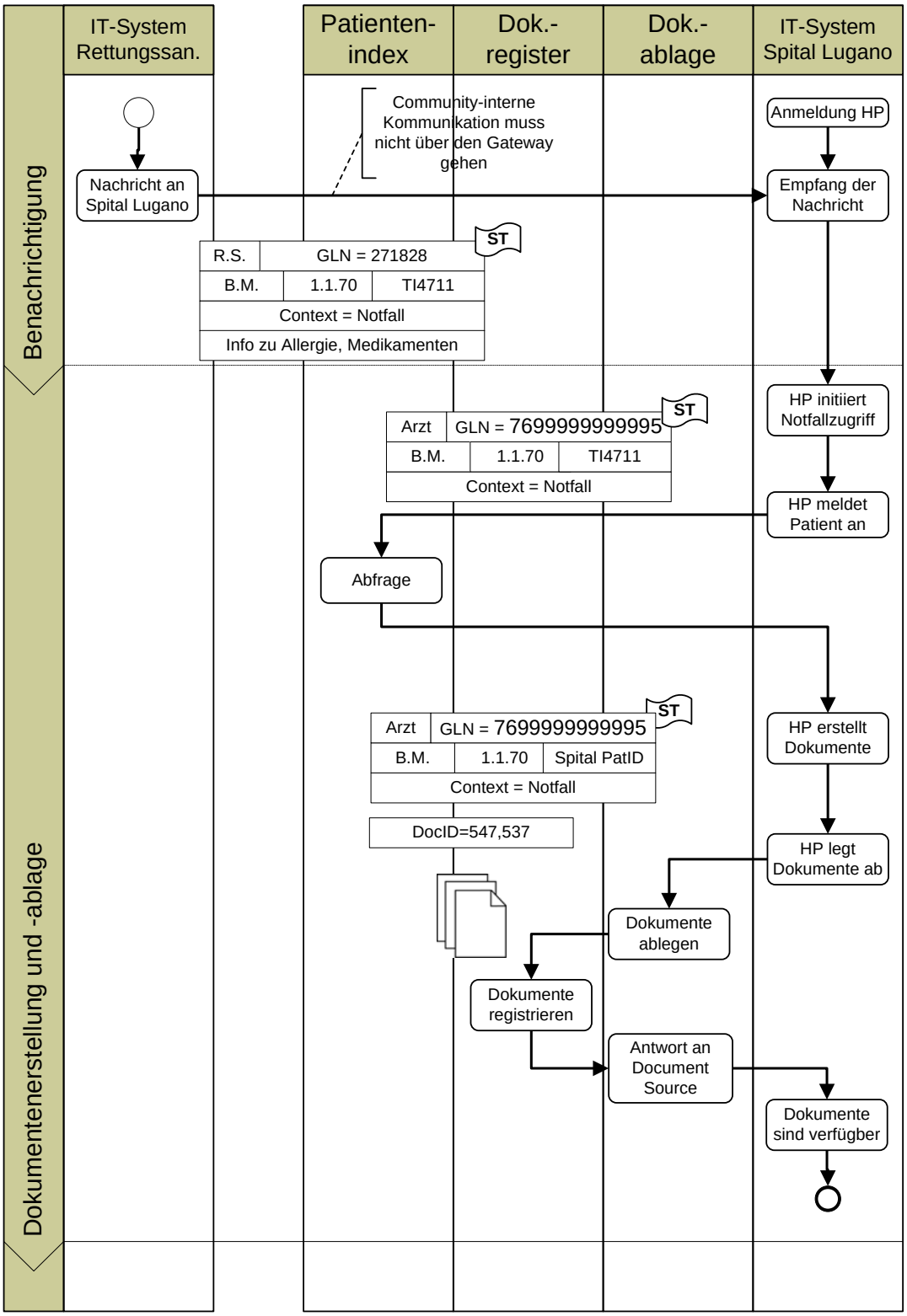
Der gewählte Ablauf für die Use case-Abwicklung nimmt eine IHE-mässige Umsetzung mit drei Schritten an (1. Suche nach Patient, 2. Suche nach Dokumenten, 3. Bezug der Dokumente). Als Alternative könnte man sich auch vorstellen, dass die Orchestration dieser drei Schritte auf Seite der angefragten Community stattfinden (evtl. sogar im Gateway). Die beiden Varianten sind wie folgt zu beurteilen.

Variante	A. „IHE-mässig“	B. „Eine Einzelquery“
Beschreibung	Drei Schritte / Iterationen zwischen anfragender und angefragter Community	Nur ein Schritt zwischen anfragender und angefragter Community
Stärken	• Einfaches Umkonfigurieren einer Community auf XCA	• Nur eine Iteration nötig (kurzer Delay)
Schwächen	• Es sind drei Iterationen über alles hinweg nötig (mit entsprechendem Traffic / Delays). • Die IDs werden entweder exposed oder müssen verschlüsselt werden.	• Keine XCPD / XCA-Schnittstelle mehr und alle Systeme sind entsprechend anzupassen.
Optionen	Verwendung einer Health Data Locator Registry	Formulieren eines neuen IHE-Profils
Empfehlung	**Die empfohlene Variante**	**Nicht empfohlen**

Tabelle 2: Umsetzungsvarianten für die Orchestration der Schritte gemäss IHE-Profilen

Fortsetzung des Use Cases (Fortsetzung der Behandlung im Spital Lugano):

alles in Community TI



3.4 Use case 12 „Behandlungsauthentisierung”

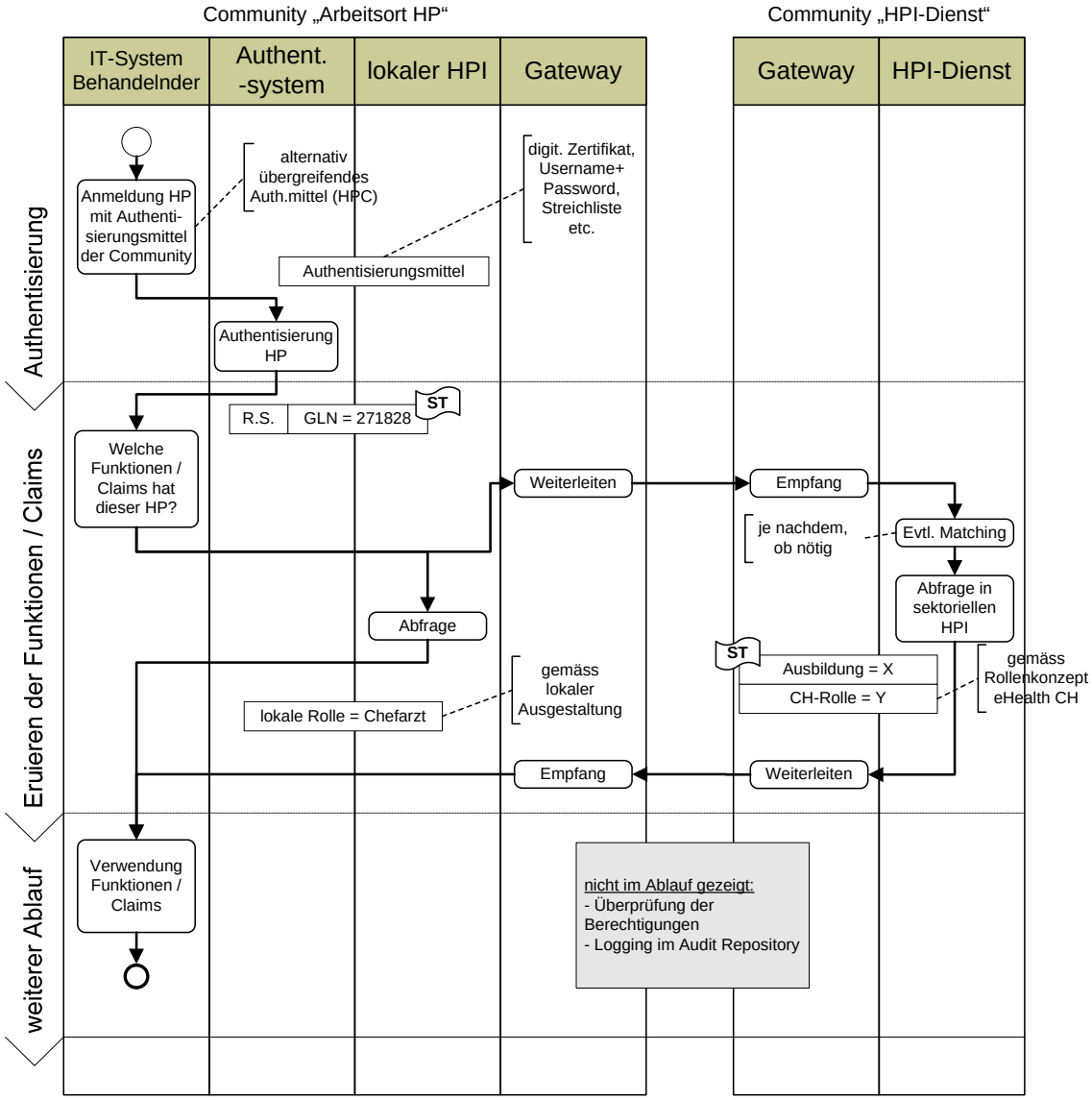
Beschreibung des Use cases [UseCaseDokument]:

Annahmen:
Ein Health Professional könnte über mehrere Authentisierungsmittel (z.B. verschiedene Karten) in verschiedenen Domänen verfügen.

Beschreibung:
Ein Health Professional meldet sich bei einer Domäne mit einer HPC an.

Variationen:
1. Ein Health Professional praktiziert in unterschiedlichen Domänen
   a. mit denselben Authentisierungsmitteln
   b. mit unterschiedlichen Authentisierungsmitteln

Akteure:
Health Professional



Es sind zwei prinzipielle Varianten für das Authentisierungsmittel der Behandelnden denkbar: lokale Mittel (z.B. Spital-Badge) oder ein übergreifendes Mittel (z.B. HPC oder SuisseID)
→ für eine Diskussion dieser beiden Varianten siehe Tabelle 17 auf Seite 62.

3.5 Nächste Schritte / offene Punkte

Titel	**Illustration der Use cases anhand der Resultate aller drei Mandate**
Details	Erstellung von genauen Ablaufdarstellungen, wie die Use cases abzuwickeln wären – unter Berücksichtigung aller drei Mandate: Basiskomponenten (vgl. Illustrationen in diesem Kapitel), Rollenkonzept (strukturelle und funktionale Rollen, Konzept von Primär- und Sekundärsystemen) sowie Metadaten. Idealerweise auch gemeinsam mit Ausgestaltung des Berechtigungssystems.

4 IT-Infrastruktur (inkl. Anbindung und Austausch)

Abgrenzung:

Gemäss Absprache mit dem Koordinationsorgan eHealth Bund-Kantone enthält dieses Kapitel nur Anforderungen, Hinweise und Abgrenzungen.

Die IT-Infrastruktur ermöglicht das Zusammenspiel / die Interoperabilität der Elemente in den Communities. Für die Ausgestaltung der Netzwerkinfrastrukturen innerhalb der Communities werden keine Vorgaben gemacht.

4.1 Architektur IT-Infrastruktur

Aufgaben:
- Anbindung der Gateways der Communities
- Weiterleiten von Nachrichten von Gateway zu Gateway
- *Mögliche weiter gehende Funktionalität siehe Kapitel 4.2*

Design-Anforderung:
- Anbindung der Community-Gateways über gesicherte Verbindungen
- Angemessene Performance des Gesamtsystems (Durchsatz, Delays etc.)
- Einhalten der Sicherheitsanforderungen
  - Vertraulichkeit der Nachrichten
  - Integrität der Nachrichten
  - Verfügbarkeit
- Für Varianten der Ausgestaltung: siehe Tabelle 3 auf der folgenden Seite.

Anforderung an die Anbindung einer Community an die IT-Infrastruktur (diese Anforderungen sind zu erfüllen bevor eine Anbindung erfolgt):
- Ausgestaltung des Gateways gemäss Design-Vorgaben (siehe weitere Kapitel)
- Ausgestaltung von weiteren in der Community geforderten Elementen (siehe Kapitel 2.3 bzw. Verweise darin)
- Aufsetzen einer angemessenen Betriebs-/Service Management-Organisation
- Erfüllung Mindestanforderungen Informationssicherheit (z.B. analog ISO-17799)

Im Kontext des in Kapitel 2 gezeigten Gesamtbilds der Architektur lässt die oben genannte Ausgestaltung der IT-Infrastruktur die in folgender Tabelle gezeigten Varianten zu.

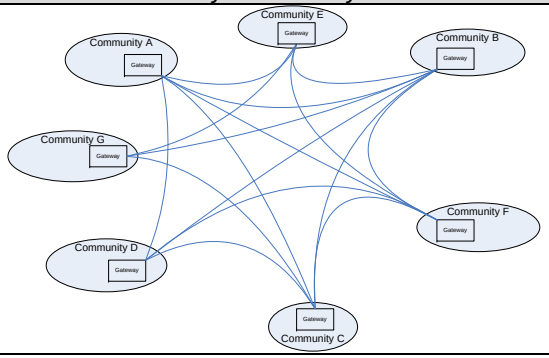
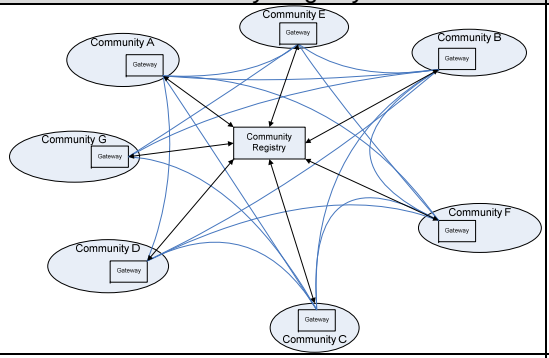
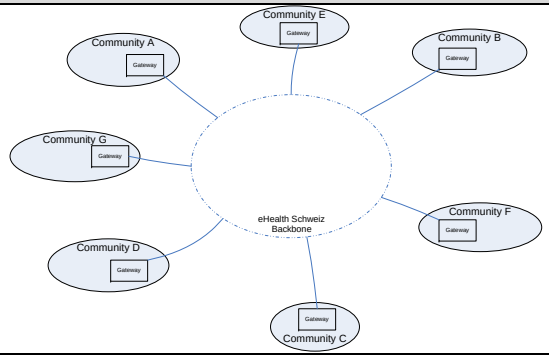
Variante	A. Rein Community-Community	B. Zentrale Community Registry	C. eHealth Schweiz Backbone
Illustration			
Beschreibung	Die Communities kommunizieren ausschliesslich direkt miteinander. Jede Community kennt alle anderen Communities.	Eine zentrale Community Registry führt ein Verzeichnis aller Communities sowie weitere gemeinsam relevante Informationen. Die eigentliche Datenkommunikation erfolgt anschliessend direkt.	Ein gemeinsamer Backbone / Server stellt die Anbindung und den Datenaustausch zwischen den Communities sicher. Sämtliche Kommunikation zwischen Communities erfolgt über diese Infrastruktur. Der Backbone kann auf der bestehenden Telematikinfrastruktur aufgebaut werden.
Stärken / Opportunities	• Keine zentralen Elemente (ausser eine Community hat eine zentrale Bedeutung – wie z.B. der NCP)	• Zentrale Community Registry als Abfrageort für zentral nötige Informationen. • Neue Communities werden einfach zur Community Registry ergänzt. • In beschränktem Masse zentrales Logging möglich	• Neue Communities binden sich einfach mit ihrem Gateway an diesen Backbone an. • Nur N Verbindungswege • Zentral nötige Informationen / Elemente können im Backbone sein. • Möglichkeit, weitergehende Funktionalität anzubieten (siehe Kap. 4.2)
Schwächen / Risiken	• Alle gemeinsam genutzten Informationen müssen zu allen Communities verteilt werden (speziell z.B. wenn eine neue Community beitritt) • N*(N-1) Verbindungswege	• Es gibt keine Möglichkeit, den Verkehr zwischen den Communities zu verfolgen / dazwischenzugreifen bzw. übergreifende Berechtigungen sicherzustellen. • N*N Verbindungswege	• Single-Point-of-Failure, sehr hohe Performance- und Verfügbarkeitsanforderungen
Fazit	**Nicht empfohlen**	**Empfohlen, falls Dezentralität im Fokus**	**Empfohlen, falls zentrale Kontroll-möglichkeiten gewünscht**

Tabelle 3: Varianten zur Ausgestaltung der IT-Infrastruktur

4.2 Mögliche weiter gehende Funktionalität der IT-Infrastruktur

Die in Kapitel 4.1 aufgeführten Aufgaben der IT-Infrastruktur stellen nur die Grundanforderungen dar. Darüber hinaus sind die folgenden Funktionen in einer gemeinsamen IT-Infrastruktur denkbar.

Zu den Vorschlägen: Die folgende Aufstellung führt mögliche weiter gehende Funktionalitäten auf und beurteilt diese kurz. Es ist im Detail zu analysieren / diskutieren, welche dieser Elemente schlussendlich zur Umsetzung zu empfehlen sind.

Für alle aufgeführten Elementen/Funktionen gilt in der Regel:

- Es handelt sich um eine Verschiebung von Funktionalität aus den Communities (typischerweise aus den Gateways), welche ohnehin umgesetzt werden muss.
- **Die Alternativvariante ist also jeweils die Umsetzung der angegebenen Funktionalität als Aufgabe der Community (typischerweise des Gateways)**

Folgende allgemeine Beurteilung der einzelnen Elemente / Funktionen kann festgestellt werden:

- Vorteile:
  - Synergien bei der Umsetzung: statt N-mal in den Communities nur einmal gemeinsam
  - Sicherstellung der Umsetzung: statt N Audits muss nur einer durchgeführt werden
  - Stärkung der übergreifenden Steuerung
- Nachteile:
  - Besondere rechtliche Grundlagen zu schaffen
  - Schaffung von Single-Point-of-Failures, sehr hohe Sicherheitsanforderungen
  - Potentiell schwierig zu realisieren (Akzeptanz, Organisation)

Element / Funktion	Beschreibung	umsetzbar mit		Beurteilung
		Community Registry	Backbone[9]	
Logging der Kommunikation zwischen den Communities	Protokollierung des Verkehrs zwischen den Communities (in Ergänzung zum Logging in den Gateways)	(X)	X	Vorteil: Bereitstellung eines zentralen Audit-Repositories → einfachere übergreifende Transparenz Nachteil: Rechtliche Grundlagen zu schaffen Sehr hohe Sicherheitsanforderungen
Durchsetzen von Berechtigungen / Policies	Die zentrale Drehscheibe könnte durchsetzen, welche Community mit welcher anderen welche Informationen austauschen kann. Könnte z.B. bei einer Integration von „Dritten“ wie z.B. Versicherungen oder von Pharma interessant werden.	(X)	X	Vorteil: Einfaches Durchsetzen von Berechtigungsvorgaben Nachteil: Sehr hohe Sicherheitsanforderungen *Dieses Thema ist im Kontext des Berechtigungssystems zu diskutieren.*

[9] Es ist zu beachten, dass bei der vorliegenden Verwendung des Begriffs „Backbone“ die auch häufig verwendete breitere Auffassung Anwendung findet, welche über reine Aspekte der Kommunikation hinausgeht und auch Applikationsfunktionalität umfasst. Hinweis: Der aktuelle Stand des Rollenkonzeptes vom 9.4.2010 verwendet eine engere Definition, welche sich nur auf Kommunikation beschränkt.
Es ist auch zu ergänzen, dass es sich je nach Funktion um mehrere Backbones handeln kann.

Element / Funktion	Beschreibung	umsetzbar mit		Beurteilung
		Community Registry	Backbone[9]	
Service-Verzeichnis	Verzeichnis von Communities und angebotenen Services	X	X	Vorteil: Service-orientierte Architektur Nachteil: Sehr hohe Sicherheitsanforderungen
Health Data Locator	Führen von Informationen, in welchen Communities Patienten bekannt sind, damit man nicht alle Communities einzeln abfragen muss (z.B. mittels XCPD Health Data Locator Option)	X	X	Vorteil: Schnellere Suche nach Patienten (und damit auch nach Dokumenten) Nachteil: Rechtliche Grundlagen zu schaffen Sehr hohe Sicherheitsanforderungen
Mapping von Patientenidentifikatoren	Der Backbone könnte im Sinne einer zentralen „Drehscheibe“ die verschiedenen lokalen IDs ineinander übersetzen (und dabei gleichzeitig steuern wer bzw. bei welchen Interaktionen dies gemacht werden darf).		X	Vorteil: Zusammenführung der verschiedenen lokalen IDs an ein einem Ort Viele Vorteile eines Master-Index ohne einen solchen zu haben (Akzeptanz) Nachteil: Rechtliche Grundlagen zu schaffen Sehr hohe Sicherheitsanforderungen
Mapping von Behandelndenidentifikatoren	Die zentrale Drehscheibe könnte die verschiedenen lokalen IDs bzw. sektoriellen IDs ineinander übersetzen (und dabei gleichzeitig steuern wer bzw. bei welchen Interaktionen dies gemacht werden darf).		X	Vorteil: Zusammenführung der verschiedenen lokalen IDs an einem Ort Viele Vorteile eines Master-Index ohne einen solchen zu haben (Akzeptanz) Nachteil: Rechtliche Grundlagen zu schaffen Sehr hohe Sicherheitsanforderungen
Bereitstellung gemeinsamer Metadaten	Führen, Bereitstellen und Historisieren von übergreifend verwendeten Metadaten (XDS Metadatenstrukturen und -werte, OIDs, Dokumentenformate etc.) Dabei kann es sich um CH-spezifische Metadaten oder solche von übergeordneten Registrierungsstellen handeln.	X	X	Vorteil: Masterlisten / Strukturen / Stammdaten an einem zentralen Ort Förderung Datenqualität Nachteil:
Noch weiter gehende Elemente wären natürlich: „nationaler Patientenindex“, „nationales Dokumentenregister“ sowie „nationale Dokumentenablage“. Da jedoch klar ist, dass Akzeptanz / Umsetzbarkeit dieser Elemente im Kontext Schweiz sehr schwierig ist, wird auf eine Diskussion an dieser Stelle verzichtet.				

X = auf dieser Basis möglich
(X) = eingeschränkt / kompliziert auf dieser Basis möglich

Tabelle 4: Denkbare Funktionen/Elemente der gemeinsamen IT-Infrastruktur

4.3 Nicht-funktionale Anforderungen

Dieses Unterkapitel diskutiert kurz die nichtfunktionalen Anforderungen und Varianten, wie eine angemessene Performance des Gesamtsystem erreicht werden kann.

Allgemeine nicht-funktionale Anforderungen des Gesamtsystems sind:

- Sicherheit, Vertraulichkeit und Nachvollziehbarkeit
- Die Zugriffe auf die Patientenindizes, Dokumentenregister/-ablagen und die Audit-Logs werden vom Berechtigungssystem kontrolliert.
- Angemessen Performance (Antwortzeiten, gleichzeitige Anwender/Abfragen, Datendurchsatz)
  → *diese Anforderungen sind noch abzuschätzen*
  → *für mögliche Ansätze speziell die Antwortzeiten zu erreichen siehe Tabelle 5 unten.*
- Verfügbarkeit "rund-um-die-Uhr"
- Der Datenschutz muss gewährleistet sein.
- Historisierung der Daten (um u.a. Nachvollziehbarkeit sicherzustellen)
- Vertraulichkeit und Integrität der Daten

Nicht-funktionale Anforderungen bei Verwendung der IHE-Profile (XCPD, XCA)

- Verwendung von ATNA und CT
- Netzwerkschutzmassnahmen: XCPD Schnittstellen sind gegen Missbrauch und DoS-Attacken zu schützen.
- Überwachungsprozess für Audit-Logs ist empfohlen. Dieser soll bei unangemessenen Handlungen Alarm geben.

Varianten für das Erreichen von angemessenen Antwortzeiten

Variante	A. Keine besonderen Elemente	B. Ein gemeinsamer Health Data Locator	C. Dezentrale Health Data Locators in Zugangs-Community
Beschreibung	Es werden keine besonderen Vorkehrungen für Beschleunigung von Abfragen getroffen.	Ein gemeinsamer Health Data Locator speichert, in welchen Communities Daten zu Patienten vorhanden sind.	Die jeweiligen Zugangs-Communities führen eine Verzeichnis, in welchem Communities Daten zu bestimmten Patienten vorhanden sind.
Stärke	• Einfach umzusetzen • Keine Datenschutzbedenken	• Technisch relativ leicht umzusetzen (in der IT-Infrastruktur) • Einfach mit Berechtigungsverwaltung zu kombinieren (in der IT-Infrastruktur)	• Technisch relativ leicht umzusetzen (in Zugangs-Community) • Einfach mit Berechtigungsverwaltung zu kombinieren (in Zugangs-Community)
Schwäche	• Performance begrenzt / potentiell sehr lange Antwortzeiten	• Datenschutzbedenken	• Der schnelle Zugriff auf Daten eines Patienten muss über die jeweilige Zugangs-Communitiy erfolgen. • Mehrfache Datenhaltung / zusätzlicher Traffic (falls ein Patient bei mehreren Zugangs-Communities ist)
Fazit	**vermutlich nicht performant genug**	**die optimale Variante, falls gemeinsames Element möglich ist**	**die einzige Variante, falls nur dezentrale Ausgestaltung möglich**

Tabelle 5: Varianten für das Erreichen von angemessenen Antwortzeiten

4.4 Nächste Schritte / offene Punkte

Titel	Wahl der grundlegenden Variante für die IT-Infrastruktur
Details	Festlegen, welche der in Kap. 4.1, Tabelle 3, gezeigten Variante für die IT-Infrastruktur umgesetzt werden sollten.

Titel	Konkretisierung weiter gehender gemeinsamer Funktionalität
Details	Festlegen, welche der in Kap. 4.2, Tabelle 4, aufgeführten Funktionen/Element gemeinsam als Teil der IT-Infrastruktur umgesetzt werden sollten.

Titel	Analyse / Klärung der Performance des Gesamtsystems
Details	Welchen Performance-Anforderungen wird das Gesamtsystem genügen müssen? Wie lässt sich eine zufriedenstellende Gesamtperformance (speziell Antwortzeiten bei grosser Verschachtelungstiefe von Communities) erreichen? Ansätze und Variantendiskussion siehe in Kap. 4.3, Tabelle 5.

5 Berechtigungssystem

Abgrenzung:

Gemäss Absprache mit dem Koordinationsorgan eHealth Bund-Kantone enthält dieses Kapitel nur Anforderungen, Hinweise und Abgrenzungen.

Das Berechtigungssystem nimmt innerhalb der Schweizerischen eHealth-Strategie eine zentrale Rolle ein. Steht ein funktionierendes und verständliches System zur Verfügung, so steigt auch ohne Zweifel die Akzeptanz der weiteren Komponenten bei den Akteuren.
Die Grundlage für ein Berechtigungssystem können jedoch nicht ohne Vorarbeiten gelegt werden. Zwingende Voraussetzungen sind aus unserer Sicht: Das Erstellen einer eHealth Governance, welche die Steuerung und Regelung des Systems beschreibt und zweitens die Ausarbeitung eines Rollenkonzeptes. Erst wenn diese beiden Elemente vorhanden sind, kann die genaue Ausprägung eines Berechtigungssystems definiert werden. Das Berechtigungssystem steht somit zuoberst und setzt auf eHealth Governance und Rollenkonzept auf.

Empfehlung
Wir empfehlen dem Koordinationsorgan eHealth Bund-Kantone die noch fehlenden Punkte einer eHealth Governance baldmöglichst in Angriff zu nehmen, spätestens jedoch als erster Teil eines weiteren Mandates für die Definition des Berechtigungssystems.

5.1 Anforderungen

Ein Berechtigungssystem im generellen Sinn soll die folgenden Themen abdecken
- Authentisierung
- Autorisierung
- Administration
- Auditing

Es ist zu diskutieren, inwieweit Authentisierung zum einem Berechtigungssystem gehört oder ob dieses Thema nicht separat behandelt werden soll.

Aufgaben:
- Authentisierung von Behandelndem und Patient
- Ausstellen von Security Tokens zur Validierung der Identität von Behandelnden und Patienten
- Auswertung der Security Tokens zur Prüfung der Identität von Behandelnden und Patienten.
- Durchsetzen der geltenden Richtlinien und Policies
- Verwaltung der Berechtigungen durch den Patienten (funktionale Rollen und Policies) für den Zugriff auf seinen EHR.
- Schreiben und Auswerten von Audit-Logs

Design-Prinzipien:
- Das Berechtigungssystem muss bei sämtlichen Elemente der Architektur Anwendung finden, in welchen Berechtigungen auszuwerten sind.
- Ausfallsichere Umsetzung da zentrale Komponente. Ein Berechtigungssystem muss 24*7 zur Verfügung stehen
- Diejenige Community, die Informationen an andere Communities herausgibt muss sicherstellen, dass die definierten Richtlinien und Policies eingehalten werden. (wenn Kommunikation zwischen Communities)
- Berechtigungskonzept muss in einem föderalen Umfeld einsetzbar sein
- Es existieren nationale Leitlinien, welche minimale Anforderungen definieren
- EUA/XUA, wenn innerhalb von Communities
- XUA erweitert, wenn zwischen Communities

Bemerkung zur Architektur

Obwohl die weitere Ausgestaltung der Architektur für das Berechtigungssystem nicht Gegenstand dieses Mandats ist, erscheint uns ein Punkt zentral zu sein:
Designprinzip: Das Berechtigungssystem darf nicht durch die konsumierenden Applikationen (Document Consumers) selber umgesetzt werden, sondern muss eine Komponente sein, die unabhängig von den Applikationen ist.
Es drängt sich somit auf, eine Berechtigungskomponente „vor“ die Systeme zu setzen, welche die medizinischen Daten zu Patienten enthalten. Dies sind:

- Die Registries (inklusive Zugriff auf HPI und MPI)
- Die Repositories

Die Registry muss gesichert werden (z.B. durch einen entsprechenden Schutzwall), weil bereits die Existenz eines Dokumentes eine schützenswerte Information darstellt und ohne eine entsprechende Berechtigung nicht weitergegeben werden.
Das Repository enthält die eigentlichen medizinischen Daten und ist somit ebenfalls schützenswert.

Designprinzip: Die Anfragen an Registry und Repository müssen durch eine Berechtigungskomponente gefiltert bzw. „intercepted“ werden.

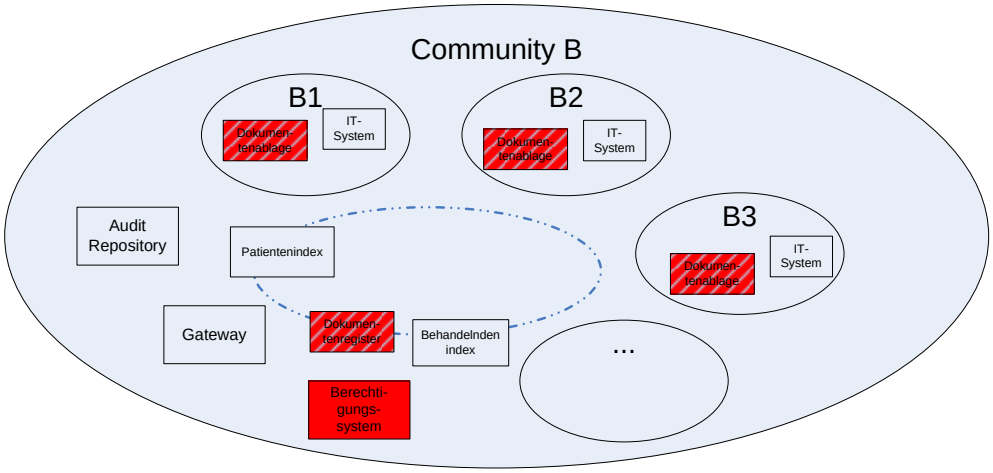


Abbildung 5: Absicherung der Registry und Repositories durch das Berechtigungssystem

Empfehlung der IHE

Im Whitepaper der IHE [ITI_WP-AccessControl] ist eine umfangreiche Diskussion zum Thema Access Control enthalten. IHE gibt die Empfehlung die Authentisierung und Autorisierung zu trennen.

Grundidee: Trennung von Authentifizierung und Autorisierung – Das Authentifizierungsverfahren liefert eine transferierbare Repräsentation des authentifizierten Benutzers (Security Token), die vom Autorisierungssystem benutzt werden kann. Ein Security Token kann die Patienten-ID oder Behandelnden-ID enthalten. Aber allein die Patienten-ID oder Behandelnden-ID, die z.B. in XDS Metadaten referenziert wird, ist kein Security Token, sondern nur eine Referenz auf den Patienten bzw. Behandelnden.

Designprinzip: Berechtigungssystem separiert von anderen Komponenten (z.B. zusätzlicher Layer bzw. Interceptor vor anderen Komponenten, andere Komponenten sind nicht für Berechtigungen zuständig).

5.2 Nächste Schritte / offene Punkte

Titel	Erstellen eHealth Governance
Details	Welche Entscheidungsmechanismen stellen die Ausgestaltung und Operationalisierung im Sinne Strategie eHealth Schweiz sicher? Konkret: Wer entscheidet was? Wer liefert Input und wer kann Entscheidungsvorschläge formulieren? Wie sehen die Entscheidungsabläufe aus?

Titel	Konzeption Berechtigungssystem
Details	Konkrete Ausgestaltung des Berechtigungssystems im Kontext der eHealth Governance, des Rollenkonzeptes und der Basiskomponenten. Fragen, die es zu klären gilt: • Auf welcher Ebene werden die Berechtigungen definiert (Schweiz weit, kantonal, regional, sektoriell? • Auf welcher Ebene werden die Berechtigungen verwaltet (Schweiz weit, kantonal, regional, sektoriell, Berufsverbände, pro LE, pro Patient? • Wer verwaltet die Berechtigungen (Bund, Kantone, Regionen, Sektoren, Einzelne Institutionen, Patient)? • Berechtigungskonzept im Notfall • Rolle des Confidentiality Codes (im Moment einfach ein Attribut in den Metadaten) • Wie ist das Lifecycle Management von Berechtigungen geregelt? Z.B. Austritt eines Arztes • Temporale Berechtigungen (Stages in einer Arztpraxis, Unterassistenten) • Welche Rechte gelten in einem community-übergreifenden Szenario?

6 Patientenindex

Im Themenbereich „Patientenindex“ soll die Architektur den Zusammenhang zwischen Identifikatoren und Indizes (Verzeichnissen) sowie die Verbindung zwischen verschiedenen parallel geführten Indizes aufzeigen.

In diesem Kapitel werden drei Themen speziell behandelt:

- **Patientenindex:** Der Patient wird in einem Index geführt
- **Patientenidentifikation:** Der Behandelnde identifiziert einen Patienten
- **Authentisierung:** Der Patient wird authentifiziert (Abgrenzung zu Berechtigungssystem)

6.1 Architektur

Patientenindizes sind Teil der Communities. Es ist keine übergreifende Umsetzung im Sinne eines Schweiz weiten Patientenindex erforderlich.

Die folgende Abbildung illustriert die prinzipielle Architektur und den Zugriff über Communities hinweg.

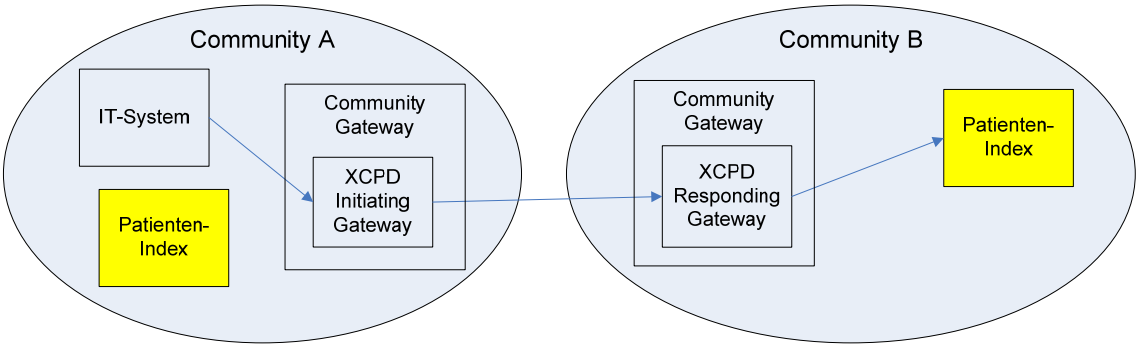


Abbildung 6: Patientenidentifikation über Communities hinweg

Ein Patientenindex einer Community wird für andere Communities über einen Gateway zur Verfügung gestellt.

6.1.1 Details Patientenindex

Der Patientenindex stellt ein Verzeichnis der Patienten in der Community zur Verfügung.

Aufgabe

- Patient registrieren und unter einer lokalen Patienten-ID ablegen
- Administrative Patientendaten / demografische Daten historisiert verwalten
- Patient suchen anhand demografischer Daten / Merkmalen oder lokaler Patienten-ID

Designprinzipien

- Eine Patienten-ID ist einer Person in einem bestimmten Bereich dauerhaft eindeutig zugeordnet.
- Eine Patienten-ID wird durch eine Assigning Authority zugeteilt.
- Jede Assigning Authority hat eine weltweit eindeutige Identifikation (OID).
- Zur eindeutigen Identifikation eines Patienten muss die Patienten-ID und die OID der entsprechenden Assigning Authority angegeben werden.
- Patientendaten sollten von hoher Datenqualität sein und möglichst Merkmale für ein sicheres Matching enthalten (siehe Diskussion unten).
- Einer Person können lokal auch mehrere Patienten-IDs zugeordnet sein (z.B. falls der Patient nicht identifiziert werden konnte, als die Daten angelegt wurden).
- Patientendaten werden lokal verwaltet.

- In einer Community kann es mehrere Patientenindizes geben.
- In einer Community können mehrere Assigning Authorities (Patientenidentifikationsdomänen) benutzt werden.
- In einer Community kann es einen Master Patient Index (MPI) geben.
- Ein Patientenindex kann an einen XCPD-Gateway angebunden werden.

6.1.2 Merkmale der Patienten im Index

Ein Patientenindex ist ein Verzeichnis von Patienten. Im Patientenindex sind demografische und administrative Daten eines Patienten mit einer lokalen Identifikation verknüpft abgelegt. Beispiele können sein (nicht abschliessende Liste):

Merkmal	Details / Möglichkeiten
Identifikator	
Identifikator	AHVN13 oder kryptografische Ableitung (Hash)
Demografische Daten	
Name, Vorname	für hohe Datenqualität wäre wichtig: Name gemäss amtlichen Ausweis
Name bei Geburt	
Geschlecht	
Geburtsort	
Heimatland	
Telefonnummern	
E-Mail-Adressen	

Tabelle 6:Mögliche Merkmale der Patienten im Index

Es sollten solche Merkmale gespeichert werden, die eine möglichst eindeutige Identifikation der Person zulassen.

Da sich der Name einer Person ändern kann, könnte ein Schweiz- oder weltweit eindeutiges Merkmal die Identifikation einer Person erleichtern. Für Abrechnungszwecke darf bei entsprechender rechtlicher Grundlage die AHVN13 (verwaltet durch die Zentrale Ausgleichsstelle ZAS http://www.zas.admin.ch) benutzt werden, die aber nur für Einwohner der Schweiz verfügbar ist.

Auf Grund der fehlenden gesetzlichen Grundlagen und aus Datenschutzgründen ist eine Nutzung der AHVN13 im Zusammenhang mit medizinischen Daten nicht empfehlenswert.

Die folgende Tabelle diskutiert und beurteilt mögliche Varianten.

Variante	A. eindeutiges Merkmal	B. in der Gesamtheit eindeutiges Set von Merkmalen	C. ad-hoc / lokal unterschiedlich
Erläuterung	wäre quasi eine CH-Patienten-ID	Forderung eines quasi eindeutigen Sets von Merkmalen (Ansatz Registerharmonisierung)	jede Community speichert nach eigenem Ermessen Merkmale
Umsetzungsszenarien	Variante: Kryptographische Ableitung[10] Variante: Neue dedizierte CH-Patienten-ID	noch im Detail zu analysieren (z.B. Name, Geburtsname, Geburtsdatum etc.)	
Stärken	• würde viele Probleme schnell lösen • Weniger Falschzuordnungen (da die Daten eindeutig mit Person verknüpft sind - ohne falsch-positive Zuordnungen) • Dadurch höhere Patientensicherheit • Prüfziffer fördert Datenqualität bei manueller Erfassung • International einsetzbar	• würde übergreifende Interoperabilität erreichen • Bei entsprechender Stärke der Merkmale falsche Zuordnung praktisch ausgeschlossen	
Schwächen / Risiken	• Datenschutzbedenken • Akzeptanz Hinweis: Die genannten Schwächen/Risiken werden mit kryptografischer Ableitung entschärft	• Hohe Anforderungen an Datenqualität (Merkmale der CH-Versichertenkarte im Fall einer Namensänderung ungenügend, falls AHVN13 nicht zum Matching benutzt werden darf) • Definition des eindeutigen Sets von Merkmalen schwierig	• Matching von Patientendaten erfolgt in jeder Community nach anderen Regeln / Algorithmen • Dadurch Verschlechterung der Daten- und Matchingqualität • Hohe Kosten (aufgrund der Tatsache, dass es keine hundertprozentige Trefferalgorithmen gibt werden viele Personalressourcen gebunden)
Empfehlung	**die zu bevorzugende Variante (mit kryptografischer Ableitung)**	**falls Variante A nicht geht, die einzige Option**	**übergreifende Interoperabilität nur mit viel Zusatzaufwand**

Tabelle 7: Varianten zu Identifikation von Patienten

[10] Eine kryptografische Ableitung der AHVN13 wäre ein Ansatz, der im Rahmen der Entwicklung von Standards zum Matching von Personendaten betrachtet werden könnte, um die Datenqualität zu verbessern und den Datenschutz zu gewährleisten, indem falsch-positive Matches minimiert werden.

Ausgestaltung in anderen Ländern:

In den meisten **EU-Ländern** wird eine nationale Patienten-ID benutzt [epSOS-IM]. Ein bekanntes Beispiel ist **Österreich**; in **Grossbritannien** wird die Verwendung stark empfohlen [UkSaferPracticeNotice].

In den **USA** gab es Diskussionen über die Einführung eines UPI (Unique Patient Identifier). In einer Studie [Rand2008IdentityCrisis] sind die Vor- und Nachteile eines solchen Ansatzes zusammengefasst:

- UPI könnte Datenschutz verbessern (weniger falsch-positive Matches) und Qualität erhöhen (weniger Fehler beim automatischen Matching)
- UPI könnte auf freiwilliger Basis benutzt werden (Migrationspfad zu UPI – z.B. falls vorhanden von Matching-Verfahren zu benutzen, wenn Anwendung einer ID-Karte Pflicht wäre, könnte man auch später darüber UPIs in die Patientenindizes bekommen)

Im Patientenindex sollten Attribute vorgesehen werden, um die Quelle der Patientendaten zu führen bzw. die Qualität der verwendeten Daten zu dokumentieren (z.B. im Fall nicht identifizierter Notfallpatienten).

Um einen sicheren Datenaustausch auch für Personen mit Wohnsitz im Ausland zu ermöglichen (ein Fall vom Use Case 7 und relevant für das EU-Projekt epSOS), sollte ein Attribut für eine nationale Patienten-ID und ein Attribut für das Land dieses Identifikators vorgesehen werden. Es sollte spezifiziert werden, welche Merkmale von Personen benutzt werden, wenn sie keine nationale Patienten-ID ihres Heimatlandes besitzen.

6.1.3 Aufgaben des Community-Gateways im Kontext Patientenindex

Aktivitäten/Anforderungen

- standardisierte Schnittstellen (z.B. XCPD)
- Weiterleitung von Abfragen an den Patientenindex und Ergebnisse vom Patientenindex
- Zugriffe werden protokolliert

Designprinzipien

- Verbindung dezentraler Patientenindizes
- Information Hiding: Daten, die nicht über die Schnittstelle ausgetauscht werden, sind der anderen Community verborgen.
- Entkopplung: eine Community kann sich intern reorganisieren, ohne dass eine andere Community betroffen ist.

Details zur Verbindung der Patientenindizes mittels XCPD

Das IHE-Profil Cross-Community Patient Discovery (XCPD) unterstützt das Auffinden von Communities, die relevante Daten für einen Patienten halten, und die Übersetzung von Patienten-IDs zwischen Communities, die Daten zum selben Patienten besitzen.

XCPD bietet keine Möglichkeit, um Patienten in anderen Communities zu erfassen.

Eine Community kann über seinen XCPD Initiating Gateway und den XCPD Responding Gateway einer anderen Community solche Patienten suchen, die in der anderen Community bekannt sind.

Dazu können folgende IHE-Transaktionen verwendet werden:

- Die Transaktion **Cross Gateway Patient Discovery [ITI-55]**:
  - ist für Initiating und Responding Gateways zwingend
  - stützt sich auf die Annahme, dass im gewählten Umfeld Patienteninformationen gut beschrieben sind und dass **demografische Patientendaten in einer hohen Qualität** verfügbar sind.
  - verfügt über verschiedene Modi
    - **Demographic Query only**
      Der Responding Gateway prüft **lediglich auf Basis demografischer Personendaten**, ob derselbe Patient in seiner Community registriert ist.
    - **Demographic Query and Feed**
      Der Responding Gateway prüft **auf Basis demografischer Personendaten und der Patientenidentifikation des Initiating Gateway**, ob derselbe Patient in seiner Community registriert ist.
    - **Shared/national Patient Identifier Query and Feed**
      Der Responding Gateway prüft lediglich auf Basis einer gemeinsamen Patientenidentifikation, ob derselbe Patient in seiner Community registriert ist.
- Die Transaktion **Patient Location Query [ITI-56]**:
  - ist für Initiating und Responding Gateways optional
  - liefert dem Initiating Gateway eine Liste von Communities, in welchen der Patient gemäss Informationen auf dem Responding Gateway über relevante Gesundheitsinformationen verfügt.
  - wird benutzt für die Health Data Locator Option von XCPD.

XCPD spezifiziert nicht das verwendete Matching-Verfahren. Um ein Matching mit grosser Sicherheit zu ermöglichen, sollte das Verfahren für eHealth Schweiz spezifiziert werden (z.B. wie mit dem Parameter MinimumDegreeMatch umgegangen werden soll).

6.1.4 Ausgestaltungsmöglichkeiten innerhalb der Communities

In einer Community können verschiedene Patientenidentifikationsdomänen benutzt werden (z.B. Institutionen mit je einem lokalen Patientenindex). Einem Dokumentenregister ist jedoch genau eine Patientenidentifikationsdomäne zugeordnet.

Verwendung eines Master-Patient-Index
Ein Master Patient Index (MPI) ist ein Index, welcher alle Indizes eines Patienten aus verschiedenen Bereichen (Krankenhäusern, Abteilungen eines Krankenhauses, Arztpraxen etc.) referenziert. Ein MPI dient dazu, die Information aus den verschiedenen Quellen unter einer gemeinsamen Identität zusammenzuführen. Ein MPI kann benutzt werden, um Patienten-IDs zwischen Patientenidentifikationsdomänen zu übersetzen.

Ansatz der Fusion von Patientenidentifikationsdomänen mittels MPI
Patientenidentifikationsdomänen (Patient Identifier Domains) können unabhängig von XDS Affinity Domains zu einer grösseren Patient Identifier Domain fusioniert werden (unter der Annahme, dass die kleineren Patient Identifier Domains erhalten bleiben). Wenn mehrere XDS Affinity Domains eine Patient Identifier Domain gemeinsam nutzen, wird eine Fusion der XDS Affinity Domains einfacher.

Hierarchisches Zusammenführen von Communities

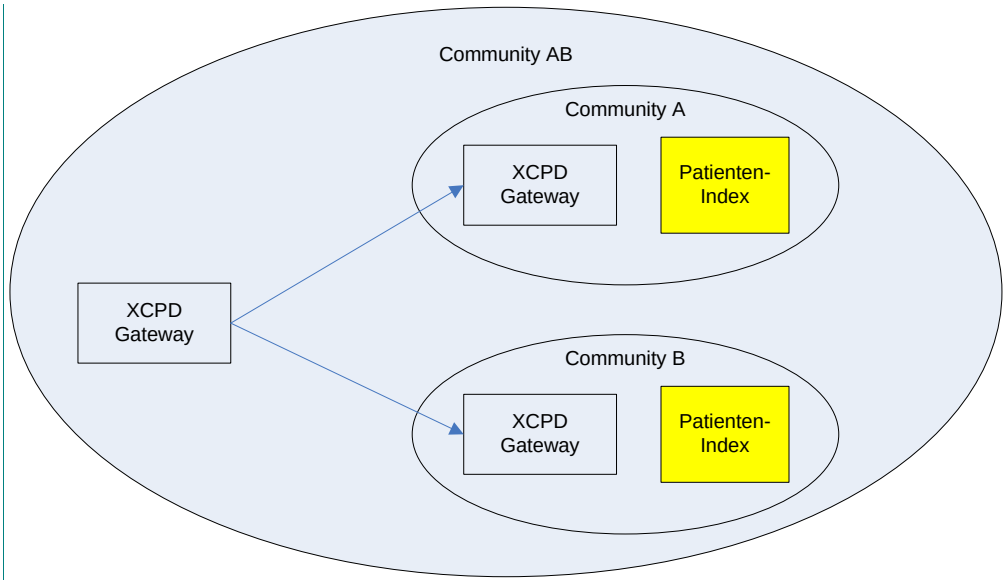


Abbildung 7 Ansatz zur Fusion von Communities mittels XCPD

Die Patientenindizes mehrerer Communities (z.B. Community A und B in der Abbildung) können über einen gemeinsamen XCPD-Gateway abgefragt werden. Auch innerhalb einer Community können so mehrere Patientenindizes benutzt werden.

6.1.5 Patientenidentifikation

Bei einer Behandlung muss der Behandelnde den Patienten identifizieren, um Daten des Patienten bei der Behandlung benutzen zu können oder die Behandlung zu dokumentieren.

Variante	A. Identifikationsmittel mit Foto	B. Identifikationsmittel ohne Foto	C. ad-hoc / lokal unterschiedlich
Umsetzungs-szenarien	Reisepass, Identitätskarte, neue Gesundheitskarte mit digitalem Zertifikat und Foto	CH-Versichertenkarte EU-Krankenversicherten-karte	Name, Geburtsdatum etc.
Stärken	• Sicherheitsmerkmal Foto, • Hohe Sicherheit gegen Missbrauch bei Kombina-tion mit Zertifikatspasswort (ohne Passwort nur Notfall-zugriffe mit entsprechenden Alerts)	• Akzeptanz	• Flexibilität
Schwächen / Risiken	• Möglicherweise Akzeptanz	• Missbrauch durch Dieb-stahl des Identifikati-onsmittels	• Missbrauch durch Identitätsdiebstahl • Unnötiger Zusatzauf-wand • Schlechte Patientensi-cherheit
Empfehlung	**Kombination von digitalem Zertifikat und Foto ist die favorisierte Variante**	**falls Variante A nicht geht, die einzige Option**	**nicht empfohlen**

Tabelle 8: Varianten für Identifikationsmittel für Patienten

Der Behandelnde kann mit den Daten vom Identifikationsmittel des Patienten im Patientenindex suchen und den korrekten Patienten im Index auswählen, so dass die Patienten-ID bekannt ist. Falls die Person noch nicht im Patientenindex existiert, so wird der Patient im Patientenindex neu registriert, seine Daten werden erfasst oder von einem Identifikationsmittel übernommen.

Da eine sofortige Identifikation nicht in allen Fällen möglich ist (z.B. bei bewusstlosen Patienten), könnte ein Patient mehrfach im Patientenindex erfasst sein.

Die genauen Prozesse für die Patientenidentifikation sollten innerhalb der Community geregelt werden. Da sich die internen Prozesse aber auf die community-übergreifende Kommunikation auswirken, sollten auch übergreifende Richtlinien entwickelt und angewendet werden.

Da durch eine eHealth-Infrastruktur der Datenaustausch erleichtert wird, gewinnt eine sichere Patientenidentifikation an Bedeutung (z.B. um den Missbrauch von Identitätsdiebstahl einzuschränken).

6.1.6 Authentifizierung eines Patienten

Wenn eine Person ihr elektronisches Gesundheitsdossier einsehen möchte, muss sie sich bei einem IT-System authentisieren. Anhand einer Authentisierungsmethode kann das System die Person authentifizieren. Wenn in einem Registrierungsprozess ein Authentisierungsmittel einer Patienten-ID sicher zugeordnet wurde, so kann das Ergebnis des Authentifizierungsprozesses ein Security Token sein, dass die Patienten-ID enthält.

Ein Authentifizierungsmittel wird bei einem Registrierungsprozess manuell einer Patienten-ID zugeordnet. Dadurch kann sichergestellt werden, dass einem authentifizierten Benutzer eindeutig eine Patienten-ID zugeordnet ist.

Anforderungen
- Ein Authentifizierungsmittel sollte dem Standard X.509 entsprechend ZertES entsprechen, damit es für die elektronische Signatur (z.B. des Patient Consent) benutzt werden kann.
- In Zukunft sollten weitere Authentifizierungsmittel und -verfahren integrierbar sein.
- Ein Patient kann mehrere Authentifizierungsmittel registrieren, so dass eine Migration auf zukünftige Authentifizierungsmittel möglich ist.

6.1.7 Identifizierung über CH hinaus / Ausland

Auf der Rückseite der CH-Versichertenkarte sind Daten der EU-Krankenversicherungskarte aufgedruckt. Anhand des Landescodes CH und der AHVN13 kann die Person weltweit eindeutig identifiziert werden.

Für die Patientenidentifikation in Nachbarländern der Schweiz ist das EU-Projekt epSOS relevant. Ziel des EU-Projekt epSOS ist der Aufbau und die Evaluation einer Serviceinfrastruktur zur Demonstration grenzüberschreitender Interoperabilität zwischen Electronic Health Record Systemen in Europa. Ein NCP (National Contact Point) sollte Zugriff auf einen nationalen Patientenindex haben.

Im Projekt epSOS enthält der Entwurf zu den Daten des Patient Summary das Pflichtfeld National Healthcare Patient ID.

6.2 Reifegradstufen

Im Folgenden Vorschläge für die Reifegradstufen der Themen dieses Kapitels.

Patientenindex

Stufe		Mindestanforderungen
A1	übergreifendes Element	Verwendung eines Merkmals, welches über die Schweiz hinaus eindeutig ist.
A2	übergreifend interoperabel	Gateway einer Community implementiert XCPD Alle Communities ans Netzwerk angebunden Standard für die Messages (Merkmale des Patienten) Standard für Matching-Algorithmus CH-weit eindeutiges Merkmal
B1	lokal integriert, standardisiert	PIX/PDQ HL7 v3 oder MPI oder XCPD CH-weit eindeutiges Merkmal
B2	lokal integriert, lokale Normen	lokal eindeutige Patienten-ID
C1	strukturiert, standardisiert	Es werden Standards für die Vergabe der Patienten-ID angewendet. Es werden Standards für die demografischen Patientendaten angewendet. Standards für Systeme
C2	strukturiert, lokal	Ein Patient wird registriert und erhält eine lokale Patienten-ID. Demografische Daten des Patienten werden unter dieser Patienten-ID gespeichert
D1	elektronisch ad-hoc	Demografische Patientendaten existieren als Dateien
D2	nicht elektronisch	Demografische Patientendaten existieren auf Papier im Patientendossier Patienten werden mit z.B. Name und Geburtsdatum identifiziert

Tabelle 9: Reifegradstufen Patientenindex

Patientenidentifikation

Stufe		Mindestanforderungen
A1	übergreifendes Element	weltweit benutzbares Identifikationsmittel (z.B. EU-Krankenversicherungskarte in Kombination mit Reisepass)
A2	übergreifend interoperabel	CH-weit benutzbares Identifikationsmittel (z.B. CH-Versichertenkarte oder Suisse ID)
B1	lokal integriert, standardisiert	
B2	lokal integriert, lokale Normen	z.B. kantonale Gesundheitskarte
C1	strukturiert, standardisiert	
C2	strukturiert, lokal	lokal benutzbares Identifikationsmittel (z.B. Barcode im Spital)
D1	elektronisch ad-hoc	
D2	nicht elektronisch	Patienten werden z.B. anhand Name und Geburtsdatum identifiziert

Tabelle 10: Reifegradstufen Patientenidentifikation

Authentifizierungsmittel Patient

Stufe		Mindestanforderungen
A1	übergreifendes Element	
A2	übergreifend interoperabel	CH-weit benutzbares Authentifizierungsmittel (z.B. CH-Versichertenkarte) mit Zertifikat
B1	lokal integriert, standardisiert	
B2	lokal integriert, lokale Normen	Verwendung eines in einem Verbund / Community einsetzbaren Authentifizierungsmittels
C1	strukturiert, standardisiert	
C2	strukturiert, lokal	Verwendung eines lokalen Authentifizierungsmittels
D1	elektronisch ad-hoc	
D2	nicht elektro-nisch	

Tabelle 11: Reifegradstufen Authentifizierungsmittel Patient

6.3 Szenarien / Abläufe

Elementare Use cases (im Kontext HL7 Rollen “Steps”):

- Patient registrieren
- Patient suchen

Zugriff allgemein

Szenario	Ausgestaltung
Zugriff aus eigener Domäne	geregelt innerhalb der Domäne
Zugriff aus eigener Community	geregelt innerhalb der Community
Zugriff von ausser-halb der eigenen Community	Siehe Illustration in Use Case 10 (Kap. 3.1)

Tabelle 12: Ausgestaltung der verschiedenen Zugriffsszenarien

6.4 Implikationen / Auswirkungen

In der Schweiz einmalige Elemente (Anforderung an Gesetzgebung)

- Registrierstelle für Communities (OID-Register)
- Registrierstelle für Patient Identifier Domains

Freiheiten für dezentrale Einheiten

Die Freiheiten der dezentralen Einheiten erscheinen auf den ersten Blick recht gross, da die Definitionen, Entscheide und Systemlandschaften innerhalb einer Community durch den Einsatz von Gateways zu anderen Communities getrennt sind.

Bei genauerem Hinschauen stellt man aber fest, dass IHE XCPD sehr wesentliche Vorgaben macht, die Auswirkungen auf ein Cross-Community-Umfeld haben:

1. IHE Profile ATNA und CT zwingend
   → gesicherter Kommunikationskanal
2. Demographische Patientendaten in einer hohen Qualität
   → Abgleich von Metadaten
   → Definition eines gemeinsamen Umfangs an demographischen Personendaten
   → Definition eines gemeinsamen Qualitätsanspruchs
   (hat Auswirkungen bis auf Stufe Erfassungsprozess eines neuen Patienten!)
3. Situationsbezogener (Query) oder automatisierter (Publish) Austausch von Patientenidentifikationen
   → dazu bedarf es einer klaren und unmissverständlichen Rechtsgrundlage!
4. Health Data Locator Option
   → dazu bedarf es einer klaren und unmissverständlichen Rechtsgrundlage!

Beurteilung 1:
Innerhalb einer Community gibt es zahlreiche Freiheiten (z.B. Wahl von Anbietern und Systemlieferanten oder Wahl von eigenen Policies).

Beurteilung 2:
Um Cross-Community etwas Brauchbares realisieren zu können, bedarf es einer gegenseitigen Abstimmung, die einschneidende Auswirkungen auf Basisprozesse und Primärsysteme haben.

Auswirkungen auf andere Basiskomponenten
Eine Patienten-ID wird im Berechtigungssystem, Zugangsportal, Dokumentenregister (in den Metadaten), in Dokumenten und beim Logging verwendet.

Wenn jeweils die lokale Patienten-ID benutzt wird, so müssen lokale Patienten-IDs verknüpft werden, um Patienten-IDs aus anderen Domänen der entsprechenden lokalen Patienten-ID zuzuordnen.
Die dabei benutzten Matching-Verfahren von demografischen Patientendaten sind meist statistische Verfahren und liefern nicht in allen Fällen sichere Zuordnungen.

XCPD spezifiziert nicht das verwendete Matching-Verfahren. Um ein Matching mit grosser Sicherheit zu ermöglichen, sollte das Verfahren für eHealth Schweiz spezifiziert werden (z.B. wie mit dem Parameter MinimumDegreeMatch umgegangen werden soll).

Identifikationsmittel (z.B. Versicherungskarte, eID) könnten Merkmale zur Erhöhung der Datenqualität oder für ein sicheres Matching von Patienten-IDs bereitstellen. Richtlinien und Standards sind notwendig, damit der Einsatz von Identifikationsmitteln die Datenqualität erhöht.

Wenn eine Patienten-ID eine Prüfziffer enthält, kann die Datenqualität bei manueller Eingabe wesentlich erhöht werden.

6.5 Nächste Schritte / offene Punkte

Titel	**Identifikation Patient: Auswahl Variante**
Details	Mit welcher Variante erfolgt die Patientenidentifikation? Falls eindeutiger Merkmalsset gewählt wird: wie wird die nötige Datenqualität sichergestellt?

Titel	**Identifikation Patient: über CH hinaus / Ausland**
Details	Wie erfolgt die Identifikation von Patienten, welche nicht in der Schweiz leben? Wie erfolgt die Identifikation von in der Schweiz lebenden Personen im Ausland? (jeweiliger Hintergrund: Zugriff auf Daten über Landesgrenzen hinweg via epSOS)

7 Index Behandelnde

In diesem Themenbereich geht um die Identifikation aller Behandelnden, welche am System eHealth Schweiz teilnehmen. Speziell geht es um einen Behandelndenverzeichnisdienst / „HPI-Dienst“ („Health Professional Index“-Dienst) für die Bereitstellung von Merkmalen / Identifikationsinformationen über die Behandelnden.

Information über Patienten vs. Information über Behandelnde:
Informationen über Patienten und Behandelnde sind von ihren Vertraulichkeitseigenschaften her leicht unterschiedlich:

- Informationen über **Patienten** sind a priori von höchster Vertraulichkeit, weil diese Informationen nötig sind, auf Patientendaten zuzugreifen.
- Für bestimmte Informationen über **Behandelnde** besteht jedoch ein gewisses öffentliches Interesse (z.B. Ausbildung, Akkreditierung etc.; z.B. „Ist diese Person wirklich ein beglaubigter Behandelnder?“).
- Denkbare Ausgestaltung:
  - Patienteninformation a priori vertraulich; möchte ein Patient Information über sich freigeben, so muss er dies explizit angeben („Opt-in“).
  - Behandelndeninformationen von öffentlichem Interesse a priori öffentlich. Möchte ein Behandelnder gewisse solche Informationen verbergen, so muss er dies explizit angeben („Opt-out“).

Für viele Merkmalen / Attribute – vor allem für persönliche Angaben – gelten jedoch für beide Arten von Informationen gleich hohe Vertraulichkeitsanforderungen.

7.1 Architektur

Die Architektur im Bereich Behandelndenidentifikation basiert auf den folgenden Systemen:

- **Behandelndenverzeichnisdienst / „HPI-Dienst“** (1x vorhanden im System eHealth Schweiz)
  Ein zentraler Verzeichnisdienst, der auf Anfrage durch berechtigte Systeme für Behandelnde, welche am System eHealth Schweiz teilnehmen, gewisse definierte Attribute/Merkmale bereitstellt.
- **Sektorielle Behandelndenverzeichnisse / „Sektorielle HPIs“** (Anzahl je nach Anzahl Sektoren)
  Bereichsspezifische Verzeichnisse, welche führende Systeme sind für Identitäten und Attribute/Merkmale von Behandelnden für bestimmte Bereiche.
- **Lokale Behandelndenverzeichnisse / „Lokale HPIs“** (je nach lokaler Ausgestaltung)
  Geographisch lokale Verzeichnisse, welche lokale Identitäten und lokale Attribute/Merkmale von Behandelnden in einer bestimmten Region führen.

Die folgende Abbildung visualisiert diese verschiedenen Systeme. Anschliessend folgen Beschreibungen der Aufgaben und Designprinzipien.

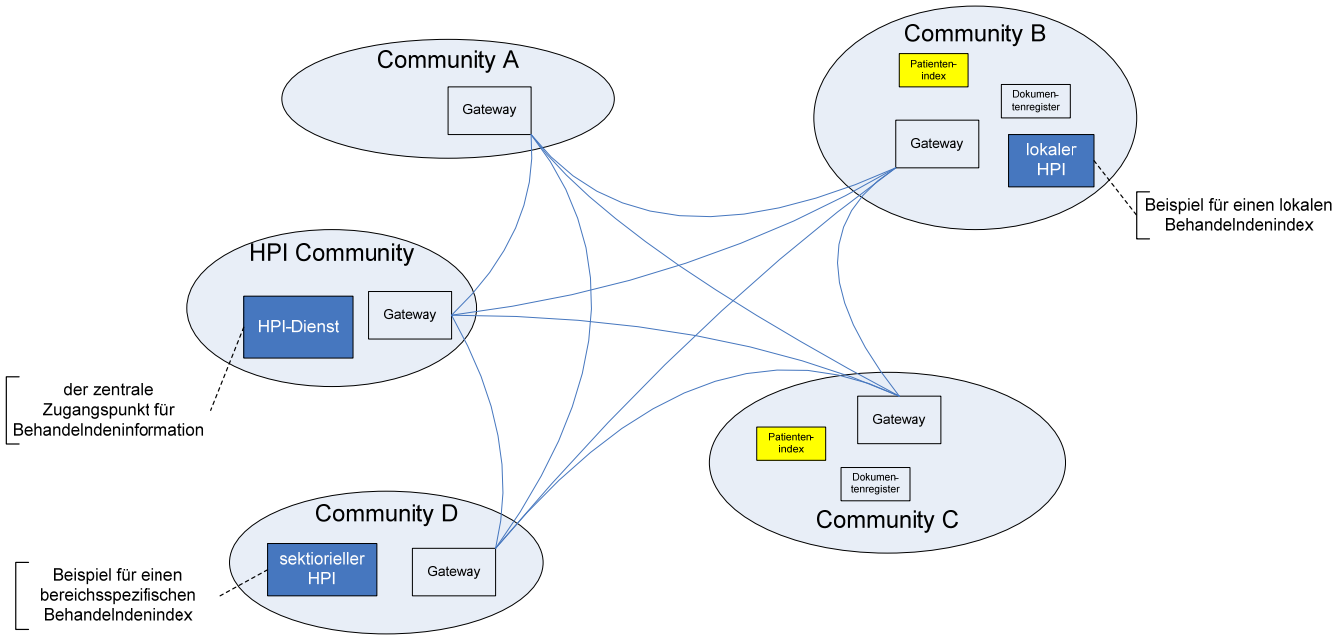


Abbildung 8: Verschiedene Arten von Behandelndenverzeichnissen / HPIs (bzw. dem gemeinsamen Dienst) im Kontext des Gesamtbildes der Architektur.

Grundsätzlich sind verschiedene Varianten denkbar, wie ein nationaler HPI-Dienst umgesetzt werden kann. Die folgende Tabelle vergleicht diese.

Variante	A. Zentraler mandantenfähiger Master-Index	B. Zentraler Index mit regelmässigen Datenlieferungen	C. Zentraler Indexdienst ohne eigene Datenhaltung
Beschreibung	In einem zentralen Verzeichnis werden alle Informationen geführt. Durch Mandantenfähigkeit können individuelle Interessen umgesetzt werden.	Ein zentrales Verzeichnis führt die Informationen als Kopien. Die lokalen / sektoriellen HPIs bleiben jedoch führend. Regelmässige Datenlieferungen halten den HPI aktuell.	Es gibt keine zentrale Datenhaltung. Die Integration der dezentralen Verzeichnisse erfolgt durch Weiterreichen der Abfragen an diese.
Mögliche Technologie	Keine geeigneten IHE-Profile OASIS: DSML, LDAP, X.500 (LDAP/X.500 empfohlen)	SOAP Messages (DSML Standard) oder Austausch von LDIF	Die IHE Profile PIX, PDQ und XCPD sind nicht nutzbar! *Umsetzungsszenarien wären zu analysieren*
Stärke	• Bewährte Technologie, mandantenfähig, könnte als Erweiterung existierender Register realisiert werden • Bei Einigung auf gemeinsame Anforderungen die günstigste Variante	• Dezentrale Verzeichnisse bleiben führend • Schnelle Antwortzeiten	• Dezentrale Verzeichnisse bleiben führend
Schwäche	• Akzeptanz bei den Beteiligten nötig • Gesetzesgrundlage zu schaffen • Komplexe Organisation / Bewirtschaftung	• Redundante Umsetzung (einmal zentral, N mal dezentral)	• Vertragliche Vereinbarungen nötig • Komplexer Authentisierungsprozesse • Am teuersten / komplexesten in der Umsetzung
Fazit	**nicht realistisch (auf Grund der komplexen Zuständigkeiten und Anforderungen)**	**empfohlene Option, falls zentrale Haltung von relevanten Informationen möglich**	**einzig verbleibende Option falls nur dezentrale Datenhaltung möglich**

Tabelle 13: Varianten für die Ausgestaltung des HPI Schweiz

7.1.1 Details Behandelndenverzeichnisdienst / HPI-Dienst

Aufgaben (in Bezug auf Behandelndeninformation)

- Der HPI-Dienst ist ein Verzeichnisdienst, der für alle Behandelnde, die am System eHealth Schweiz teilnehmen, gewisse definierte Attribute/Merkmale führt und bereitstellt.
- Zwei Arten der Nutzung:
  - interaktive Nutzung (durch Menschen; typischerweise durch ein Web-Interface)
  - transaktionelle Nutzung (durch andere Systeme; typischer durch Service-Aufrufe)
- Die Attribute/Merkmale können umfassen
  - Demographische Angaben (z.B. Name, Adresse etc.)
  - Personenidentifikatoren (z.B. GLN)
  - Offizielle Bestätigungen für qualifizierte Ausbildungen
  - Zuordnung von strukturellen Rollen gemäss Rollenkonzept zu Behandelnden
  - Weitere Merkmale wie Zugehörigkeit zu bestimmten Gesundheitsinstitutionen sind möglich

  Für eine detaillierte Liste möglicher Merkmale siehe Kap. 7.1.4.
- Der HPI-Dienst dient nicht zur Authentifizierung eines Behandelnden, sondern zur Bestätigung von Behauptungen / „Claims“ über einen bestimmten Behandelnden.

- In der Terminologie des Identity und Access Managements bildet eine solche Auskunft eines HPI-Dienstes einen sogenannten „Claim“, also eine Behauptung über einen Behandelnden.
- Ein Verzeichnis, welches solche Claims vorhält, wird „Claim Provider“ genannt.

Aufgaben (in Bezug auf Institutionsinformation):
- Bereitstellen von Informationen über Gesundheitsinstitutionen.
  Für eine detaillierte Liste möglicher Merkmale siehe Kap. 7.1.4
- Offen: Zuordnung von Behandelnden zu Institutionen (evtl. inkl. deren Funktion in der Institution)

Behandelnde vs. Provider – Ausdehnung des Scope / Kontext neues IHE-Profil HITPR:
- Stellt der HPI-Dienst nicht nur Informationen über Behandelnde sondern auch über Institutionen bereit, so ist der Begriff „Behandelnde“ zunehmend limitiert.
- Es gibt ein in Diskussion befindliches aber noch nicht verabschiedetes **IHE Profil HITPR (Health-IT Provider Registry):**
  - Ein Provider kann sowohl ein Behandelnder als auch eine Gesundheitsinstitution sein.
  - Die Provider werden klassifiziert nach Art (nach Arzt, Spital, Labor, Apotheke etc.), Personen nach Befähigung (Chirurg, Hebamme etc.), Institutionen nach Typ (administrative Stelle, Behandlungsstelle, Ort mit zugreifbaren medizinischen Patientendaten etc.)
  - Der HPI soll ein Verzeichnis aller Gesundheitsinstitutionen enthalten
  - Die Beziehungen der Behandelnden zu den Institutionen soll abgebildet und historisiert werden
- HITPR adressiert auch verschiedene Themenbereiche, welche nicht im Kontext Behandelndenidentifikation stehen und deshalb an dieser Stelle nicht behandelt werden (z.B. Bereitstellung Terminologie, Zugangspunkt für Services).
  Diese Themen sind in Gegenstand der Diskussion von Tabelle 4 auf Seite 37.

Design-Prinzipien:
- Der HPI-Dienst stellt einen zentralen Zugangspunkt für Informationen in weiteren, dezentralen Quellen dar.
- Historisierung aller Einträge (es wird nichts gelöscht, sondern nur als gelöscht markiert)
- Ein HPI muss autoritative Information enthalten, so dass eine Anfrage über einen Health Professional zu einer vertrauenswürdigen Antwort führt.
- Dementsprechend ist der Registrierungsprozess, durch welchen Einträge in datenliefernden HPI erstellt werden, genau mit den zuständigen Organisationen geregelt.
- Positionierung innerhalb des Gesamtbildes
  - In der Schweiz gibt es genau einen HPI-Dienst mit dieser Funktion
    Lokale/sektorielle HPI, welche die führenden Systeme für diese Behandelndeninformationen sind, kann es beliebig viele geben.
  - Der HPI-Dienst kann in einer eigenen dedizierten Community sein. Er kann jedoch auch Teil einer Community mit weiteren Funktionen sein. In jedem Fall wird er über einen Gateway an das Gesamtsystem angeschlossen.

7.1.2 Sektorielle HPI

Sektorielle HPI sind dezentrale Verzeichnisse (z.B. von Berufsverbänden), welche die autoritativen Personendaten halten.

Aufgaben:
- Halten der autoritativen Personendaten
- Bereitstellung dieser Daten an den HPI Schweiz

Design-Prinzipien:
- Die Bereitstellung der Daten der sektoriellen HPI an den HPI Schweiz erfolgt je nach Variante durch Datenlieferungen oder als Abfragemöglichkeiten (vgl. Tabelle 13 weiter vorne)

7.1.3 Lokale HPI

Lokale HPI sind typischerweise Teil des lokalen Identity and Access Managements (IAM) und verwalten spezifische bzw. lokale Attribute/Merkmale von Behandelnden.

Aufgaben:
- Verwalten von spezifischen bzw. lokalen Attribute/Merkmale von Behandelnden.
- Bereitstellung dieser Daten für das lokale IAM-System

Design-Prinzipien:
- Ausgestaltung nach lokalen Anforderungen
- Typischerweise nicht mit HPI Schweiz integriert (vermutlich bis auf Verwendung gewisser gemeinsamer Attribute/Merkmale)

7.1.4 Im HPI-Dienst bereit gestellte Merkmale

Die folgende Tabelle führt Merkmale von Behandelnden auf, welche der HPI-Dienst bereitstellen könnte bzw. sollte.

Zu den Vorschlägen: Es ist zu diskutieren / bewerten / entscheiden, welche Merkmale nun genau bereitgestellt werden sollen. → die aufgeführte Liste ist als ein List *möglicher* Merkmale zu sehen → es ist zu unterscheiden, welche Merkmale vorhanden sind und für welche Zwecke/Abfragen sie jeweils verwendet werden

Merkmale Behandelnde

Merkmal	Details / Möglichkeiten	Bemerkung
Bereich Identifikation		
Identifikator	• GS1 GLN (EAN) → eindeutig • AHVN13 →eindeutig, jedoch noch ohne rechtliche Grundlage • Weitere lokale Identifikatoren	Vgl. Diskussion in Kap. 7.1.5
Bereich demografische Daten		
Anrede		
Titel		
Vorname, Name, Name bei Geburt		Name bei Geburt ist sehr wichtig für das eindeutige Matching (vgl. Diskussion in Kap. 7.1.5)
Adresse	Strasse/Nr., PLZ, Ort	Welche Adresse (Wohnsitz, Arbeitsort etc.)?
Geburtsdatum		
Todesdatum		vgl. Ausgestaltung in Australien

Merkmal	Details / Möglichkeiten	Bemerkung
Bereich Ausbildung / Rollen / Spezialisierung		
Eidgenössisches oder anerkanntes ausländisches Diplom		
Strukturelle Rollen gemäss Rollenkonzept		
Spezialisierungen		

Tabelle 14: Mögliche im HPI-Dienst bereitgestellte Merkmale zu Behandelnden

Beurteilung:
Im Gesamtkontext Interoperabilität des Systems eHealth-Schweiz wird im Minimum Folgendes benötigt:
1. Genug Merkmale für eine eindeutige Identifikation (siehe Kap. 7.1.5)
2. Strukturelle Rollen gemäss Rollenkonzept

Merkmale Gesundheitsinstitution

Merkmal	Details / Möglichkeiten	Bemerkung
Angaben zur Gesundheitsinstitution		
GLN Nummer der Gesundheitsinstitution		
Unternehmens-Identifikationsnummer UID		Das Betriebs- und Unternehmensregister (BUR) des BFS ist das Basisregister für die UID. (öffentlich zugänglich. nur für Identifikation)
Klassifikation	z.B. administrativ oder klinisch	vgl. Ausgestaltung in Australien
Leistungserbringende Organisation	z.B. Typ, Service Typ, Service Unit	vgl. Ausgestaltung in Australien
Name		
Anschrift		
Angaben für elektronische Kommunikation		vgl. Ausgestaltung in Australien

Tabelle 15: Mögliche im HPI-Dienst bereitgestellte Merkmale zu Gesundheitsinstitutionen

Beurteilung:
- Mit der eindeutigen Identifikationsnummer (GLN und/oder UID) liegt eine wichtige Grundlage für Interoperabilität vor.
- Nutzen und Use cases eines zentralen / föderierten Registers von Gesundheitsinstitutionen müssen jedoch erst noch vor einer Konkretisierung definiert werden.

Verknüpfung Behandelnde – Gesundheitsinstitutionen

Verschieden Merkmale / Varianten wären denkbar zur Verknüpfung von Behandelnden- und Gesundheitsinstitutsmerkmale:

- Gesundheitsinstitution(-en) als Merkmal beim Behandelnden
- Genaue lokale Funktion des Behandelnden in der jeweiligen Gesundheitsinstitution
- Angaben zu Aufnahme und Beendigung der Tätigkeit/Funktion
- Historisierung der Merkmale

Beurteilung:
Nutzen und Use cases einer derartigen Verknüpfung müssen vor einer Konkretisierung noch definiert werden.

Hintergrundinformation: Ausgestaltung in Australien

Australien vergibt Identifikatoren an (http://www.nehta.gov.au/connecting-australia/healthcare-identifiers):

- Individual Healthcare Identifiers (IHIs) will be given to all Australian residents and others seeking healthcare in Australia
- Healthcare Provider Identifiers – Individual (HPI-Is) will be assigned to healthcare professionals and other health personnel involved in patient care
- Healthcare Provider Identifiers – Organisation (HPI-Os) will be assigned to organizations where healthcare is provided.

Klassifikation der Health Professionals

Quelle: http://www.nehta.gov.au/component/docman/doc_download/912-hi-service-provider-classification

Klassifikation der Health Professionals nach:

- Provider Individual Type (analog Weiterbildungstitel)
- Provider Individual Speciality (Subspezialität)
- Provider Individual Specialisation (Subsubspezialität)

Attribute der Health Professionals

Quelle: http://www.nehta.gov.au/component/docman/doc_download/872-concept-of-operations
Via http://www.nehta.gov.au/connecting-australia/healthcare-identifiers
TDS = trusted data source (vergleichbar mit FMH Ärzteverzeichnis)
Abschliessende Liste der Attribute:

- Name
- Address for registration
- Sex
- Date of birth
- Provider individual type

For HPI-Is allocated through a TDS it may include:

- Provider individual specialty
- TDS identifier
- Registration status

For all HPI-Is it may include:

- Business name (that is, the healthcare provider organisation name at which the Healthcare Provider Individual is employed or practices)
- Electronic communication details
- Provider individual specialisation
- Professional registration start date
- Professional registration end date
- Date of death (if applicable)

Klassifikation der Institutionen
Klassifikation der Institutionen nach:
- Administrative Healthcare Organisation
- Clinical Healthcare Organisation

In den Clinical Healthcare Organizations werden die eigentlichen leistungserbringenden Organisationen identifiziert:
- Healthcare Provider Organisation Type
- Healthcare Provider Organisation Service Type
- Healthcare Provider Organisation Services Units

Attribute der Institutionen
Abschliessende Liste:
- ABN (Australian Business Number), ACN (Australian Company Number) or other accepted organisation identifier
- Organisation Name (name under which the organisation operates)
- Address
- Service Type
- Electronic communication details
- Responsible Officer (RO) – individual with authority to act on behalf of the organisation
  - Name, DOB, address, electronic communication details (the last is optional)
- Organisation Maintenance Role (OMR) - individual appointed to administer HI Service functions for HPI-O
  - Name, DOB, address, electronic communication details (this last is optional)
  - Service unit
- Reference information to the Endpoint Location Services (ELS) for the HPI-O

Der Verzeichnisdienst

Ein HI-PDS (Healthcare Identifiers – Provider Directory Service) kann enthalten:
- HPI-I, HPI-I status and selected demographic details
- HPI-O, HPI-O status and selected organizational details
- HPI-O association with HPI-I(s) (where the HPI-I has consented)
- Specialties
- Contact information
- Electronic communication details

7.1.5 Identifikation Behandelnden

Die Behandelnden sind eindeutig zu identifizieren, auch wenn sie im mehreren Communities tätig sind. Analog zur Patientenidentifikation gibt es die folgenden Varianten:

Variante	A. Eindeutiges Merkmal	B. In der Gesamtheit eindeutiges Set von Merkmalen	C. Ad-hoc / sektoriell unterschiedlich
Erläuterung	wäre eine eindeutige Behandelnden-ID	Forderung eines quasi eindeutigen Sets von Merkmalen (Ansatz Registerharmonisierung)	jeder „Sektor“ speichert nach eigenem Ermessen Merkmale
Umsetzungsszenarien	Mit existierender ID: z.B. GLN	z.B. Name, Geburtsname, Geburtsdatum etc.	
Stärken	• würde viele Probleme schnell lösen • Keine Falschzuordnungen • Prüfziffer fördert Datenqualität bei manueller Erfassung • International einsetzbar	• würde übergreifende Interoperabilität erreichen	•
Schwächen / Risiken	• Datenschutzbedenken • Lebenslange ID problematisch bzgl. Identitätsdiebstahl	• Hohe Anforderungen an Datenqualität	• Matching von Behandelnden nur mit beschränkter Qualität möglich
Empfehlung	**falls realisierbar, die zu bevorzugende Variante**	**falls Variante A nicht geht, die einzige Option**	**übergreifende Interoperabilität nicht erreichbar**

Tabelle 16: Varianten zur Behandelndenidentifikation

Untersuchte Projekte und Standardvorgaben:

- Australien: „Health Care Provider Identification“:
  U.a. detaillierte Spezifikation der demographischen Datenelemente
- Kanada: Provider Registry Service:
  Äusserst Detaillierte Spezifikationen, Verwendung der HL7 Personnel Management Domain, Kombination zentraler und dezentraler Elemente
- ISO 27527: Health informatics -- Provider Identification (in Arbeit, Einsicht war nicht möglich)
- IHE HITPR (Health IT Provider Registry; in Arbeit, einsehbar): schlägt zusätzliche sinnvolle Funktionalität vor, welche ein reibungsloses Funktionieren eines e-Health Systems erforderlich ist.

7.1.6 Authentisierung und Autorisierung

Authentisierung und Autorisierung von Behandelnden erfolgt in den Communities im Rahmen der lokalen Identity und Access Management-Systemen.

Varianten sind grundsätzlich:

Variante	A. Lokales Authentisierungsmittel	B. Übergreifendes Authentisierungsmittel
Erläuterung	Anmeldung mit lokalem Authentisierungsmittel, Authentisierung durch das lokale Identity und Access Management System	Anmeldung mit dem übergreifenden Mittel am lokalen System, Authentisierung durch die lokale Applikation, welche das Root-Zertifikat des übergreifenden Mittels kennt und damit die Echtheit des Authentisierungsmittels überprüft.
Beispiel	Spital-Badge oder Username/Passwort	HPC SuisseID
Stärke	• Nur ein Authentisierungsmittel („Single-Sign-On“ für lokale Arbeit wie auch für Arbeit mit dem ePatentiendossier)	• Für alle Behandelnden das gleiche Authentisierungsmittel → eindeutige Identifikationsmerkmale integrierbar • Rollen klar trenn- bzw. zuweisbar: lokales Mittel → lokale Rollen übergr. Mittel → übergr. Rollen
Schwäche	• Wenn lokales Authentisierungsmittel (oder lokaler HPI) keine Merkmale mit eindeutigem Link zum HPI Schweiz zulassen, ist Matching nicht möglich	• Je nach Anwendungskontext müssen Behandelnde andere Authentisierungsmittel verwenden • Extra Kosten durch 2. Mittel
Empfehlung	**Nicht empfohlen (übergreifende Authentifizierung sehr aufwändig)**	**Empfohlen (übergreifende Zielerreichung stark gefördert)**

Tabelle 17: Varianten für Authentisierungsmittel Behandelnde

7.1.7 Details zur möglichen Umsetzung

Dieses Unterkapitel führt besonders interessante Details zur möglichen Umsetzung auf.

Analyse der IHE Profile PIX, PDQ und XCPD für den Identifikationsprozess von Behandelnden

- **PIX:** Das PIX Profil, welches den Funktionen eines Master Patient Index zugrunde liegt, erscheint nicht geeignet, um Behandelnde zu identifizieren. Es beschreibt Aktoren und Transaktionen, die im Wesentlichen dazu dienen, eine Identität aus multiplen, voneinander unabhängigen Verzeichnissen von Identitäten durch Vergleichsoperationen herauszufiltern und in einem übergeordneten Verzeichnis zur Verfügung zu halten. Man könnte vermuten, dass die Transaktionen Patient Identity Feed [ITI-8], PIX Query [ITI-9], und evtl. auch PIX Update Notification [ITI-10] von der reinen Funktionalität auch für einen HPI genutzt werden könnten, dies wird aber sofort durch die Tatsache widerlegt, dass mit den genannten Transaktionen eindeutig **nur HL7-ADT Messages zugelassen** sind. **Diese wiederum sind nicht geeignet, die Attribute eines Behandelnden zu transportieren!**
  Ein neues IHE Profil könnte womöglich dieselbe Transaktionslogik verwenden, müsste aber andere Messages definieren, die für die Abfrage eines HPI geeignet wären.

- **PDQ:** Das PDQ Profil mit den Transaktionen Patient Demographics Query [ITI-21] und Patient Demographics Visit Query [ITI-22] operiert ebenfalls mit rein patientenbezogenen Messages, welche definiert sind als HL7 Messages QBP^Q22 (Anfrage) und RSP^K22 (Antwort). Auch hier müssten für Anfragen an einen HPI eigene Messages definiert werden.

- **XCPD:** Das XCPD Profil eignet sich aus denselben Gründen wie für das PIX und PDQ angeführt nicht für den HPI-Dienst.

„Federated Directory Services“ Profil

Das **FDS-Profil** („Federated Directory Services“) ist in Entstehung begriffen. Es umfasst verschiedene andere Profilanträge (Okt. / Nov. 2009 erstmals eingereicht) wie z.B. das HPD Profil („Healthcare Provider Directory“), welches ein Verzeichnis sowohl für Behandelnde als auch für Gesundheitsinstitutionen definiert. Weitere Verzeichnisdienste, die unter FDS diskutiert werden, sind u.a. ein Verzeichnis aller Provider von Schnittstellen zu Implementierungen von IHE-Profilen analog zum UDDI („Universal Description Discovery and Integration“) Webservice-Verzeichnis Standard von OASIS. Das FDS Profil kann momentan noch nicht als Leitlinie herangezogen werden, aber die Anforderungen aus dem HITPR Profilantrag können allenfalls zu den hier beschriebenen Anforderungen addiert werden.
Das FDS-Profil ist sehr vielversprechend und sollte bei der weiteren Konkretisierung genauer angeschaut werden.

7.2 Reifegradstufen

Im Folgenden ein Vorschlag für die Reifegradstufen für den Index Behandelnde.

Stufe		Mindestanforderungen
A1	übergreifende Elemente	• Informationen über Behandelnde ist auf international standardisierte Art und Weise abgelegt / bereitgestellt.
A2	übergreifend interoperabel	• Ein gemeinsamer Index-Dienst ist über eine Standardschnittstelle unter einem definierten Zugangspunkt zugreifbar. • Ein Gateway mit Standardschnittstellen stellt die Anbindung an das System eHealth sicher. • Der Inhalt ist über alle Communities / Sektoren standardisiert.
B1	lokal integriert, standardisiert	• Informationen über Behandelnde können mit einer globalen ID (z.B. GLN) lokal gespeichert und lokal abgerufen werden. • Der Inhalt ist standardisiert. Austausch mit anderen Communities / Sektoren ist nicht möglich.
B2	lokal integriert, lokale Normen	• Informationen über Behandelnde können mit einer lokalen ID lokal gespeichert und abgerufen werden. • Der Inhalt ist standardisiert. • Austausch mit anderen Verzeichnissen in derselben Domäne ist möglich
C1	strukturiert, standardisiert	• Informationen über Behandelnde können mit einer lokalen ID lokal gespeichert und abgerufen werden. • Der Inhalt ist standardisiert.
C2	strukturiert, lokal	• Informationen über Behandelnde können mit einer lokalen ID gespeichert und abgerufen werden.
D1	elektronisch ad-hoc	• Verzeichnisse liegen lokal in elektronischer Form vor. Die Inhalte sind nicht standardisiert.
D2	nicht elektronisch	• Verzeichnis in Papierform

Tabelle 18: Reifegradstufen Index Behandelnde

7.3 Szenarien / Abläufe

Beim Behandelndenindex(-dienst) sind zwei Arten von Prozessen zu unterscheiden:
- Abläufe zur Datenverwaltung und
- die eigentliche Nutzung.

Abläufe zur **Datenverwaltung** (Input-Seite) bestehen aus:
- Automatisierten Datenlieferungen aus den vertrauenswürdigen Datenquellen
- Interaktiven Einträgen berechtigter Administratoren in vorgelagerten Verzeichnissen
- Zusammenführen von gleichen Personen
- Einzelne Arbeitsschritte sind:
  - Datensatz erstellen
  - Datensatz ändern
  - Datensatz in ein Verzeichnis hochladen
  - (Datensatz löschen wird bewusst ausgelassen, da wir eine Historisierung der Daten fordern.)

Die **Nutzung** (Output-Seite) besteht im interaktiven oder transaktionellen Abfragen von Datensätzen.
- Abfrage eines einzelnen Datensatzes
- Abfrage einer Liste von Datensätzen

Bemerkung: Je nach fachlicher und technischer Nutzung können diese Szenarien / Abläufe / Use cases sehr unterschiedlich aussehen. → vgl. dazu die beiden nächsten Schritte / offenen Punkte

7.4 Nächste Schritte / offene Punkte

Titel	**Konkretisierung HPI-Dienst (fachliche Sicht)**
Details	Welche Merkmale sollen genau bereitgestellt werden? - Für Behandelnde? - Für Gesundheitsinstitutionen? - Für deren Verknüpfung? Welche fachlichen Quellen (sektorielle HPIs) bleiben Master und stellen Informationen bereit? Welche Rolle spielen lokale HPIs? In welchen eHealth-Abläufen kommt der HPI-Dienst genau zum Einsatz? Welche organisatorischen/rechtlichen Grundlagen sind nötig?

Titel	**Konkretisierung HPI-Dienst (technische Sicht)**
Details	„Output-Seite“ (Geben von Informationen): Wie ist der HPI-Dienst genau auszugestalten? (Als technischer Service? Als Web-Auskunft? Als beides?) „Input-Seite“ (Bezug von Informationen): Wie kommt der HPI-Dienst zu seinen Information? (Mit periodischen Aktualisierungen? Mit „Real-time-Zugriff“? Mittels welchen Schnittstellenstandards?) Welche Ansätze für eine „Föderierung von HPI“ wären denkbar (z.B. mit dem FDS-Profil)? Wie ist der HPI-Dienst intern aufgebaut (Architektur)?

8 Dokumentenregister

Ein Dokumentenregister ist ein Verzeichnis, welches Informationen über vorhandene Dokumente eines Patienten speichert, so dass diese einfach gesucht, gefunden und adressiert werden können und dies unabhängig von ihrem effektiven Speicherort.

Innerhalb einer Community sollte es normalerweise ein Dokumentenregister geben. Gibt es mehrere Dokumentenregister innerhalb einer Community bzw. soll ein Austausch von Daten zwischen Communities erfolgen, so können die Communities über das IHE Profil XCA zusammengeführt, bzw. zusammengeschlossen werden.

8.1 Architektur

Im Sinne der Arbeitshypothese „IHE XCA“ diskutiert dieses Kapitel nur den community-übergreifenden Zugriff auf die Registry für das IHE Profil XCA. Die weiteren Anforderungen an ein Dokumentenregister sind in den IHE-Profilen bereits detailliert beschrieben und sollen hier nicht weiter ausgeführt werden.

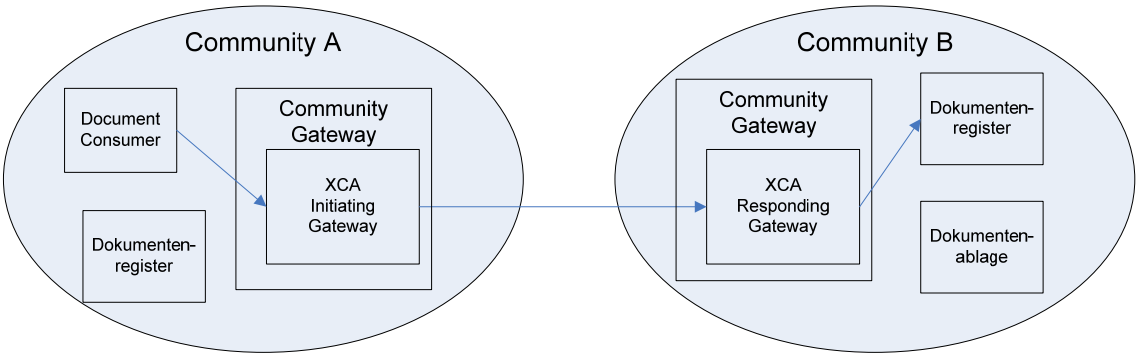


Abbildung 9: Community-übergreifender Zugriff über XCA

Anforderungen an Dokumentenregister

Aufgaben:

- Registrieren von Dokumenten mit Metadaten
- Suche von Dokumenten
  - nach Metadaten
  - mittels Dokument-ID

Designprinzipien:

- Folgende Metadaten eines Dokuments sind Minimalanforderung (um ein Funktionieren des Gesamtsystems sicherzustellen):
  - lokale Patienten-ID
  - Dokumenten-ID
  - Repository-ID
  - Behandelnden-ID
- Ein Dokumentenregister kann an einen XCA-Gateway angebunden werden
- Da im Dokumentenregister nur die Metadaten zu einem Dokument abgelegt sind, können Dokumente nicht mit einer Volltextsuche gesucht werden
- Jede Community, die XCA unterstützt, muss eine HomeCommunityID aufweisen (homeCommunityId).
- Der Zugriff auf das Document Registry wird über das Berechtigungssystem kontrolliert.

Falls in einer Community XDS Affinity Domains benutzt werden, so sind Anforderungen an das Dokumentenregister:

- Ein Dokumentenregister wird durch den Actor Document Registry des IHE-Profils XDS.b realisiert.
  - Die Transaktionen ITI-18 Registry Stored Query, ITI-42 Register Document Set – b und ITI-44 Patient Identity Feed HL7v3 oder ITI-8 [ITI TF-1] werden unterstützt.
  - Die Document Registry kann an die XCA Actors Initiating Gateway und Responding Gateway angebunden werden.
  - Die XDS-Metadaten zu einem Dokument enthalten die Patienten-ID der Assigning Authority Domain der XDS Affinity Domain [ITI TF-3].
- Die Document Registry (bzw. die XDS Affinity Domain; siehe [ITI TF-1]) unterstützt XDS-Metadaten, die einem Standard entsprechen.
  - Die zugelassenen Dokumentformate sind definiert.
  - Vokabulare und Codierschemas sind definiert.
  - Eine Patient Identification Domain ist definiert.

XCA (Cross Community Access)

Nicht alle Unternehmen sind in derselben XDS Affinity Domain zusammengeschlossen. In der realen Welt gibt es viele Affinity Domains, die aber trotzdem miteinander Daten austauschen möchten. Dank XCA können Akteure ausserhalb einer Affinity Domain über einen Gateway zugreifen mit einem minimalen Set an Transaktionen.

XCA unterstützt nur Document Consumers, d.h. es sind nur community-übergreifende Abfragen, jedoch nicht community-übergreifende Registrierungen möglich.

Anforderungen an den Gateway

Aufgaben:

- standardisierte Schnittstellen (XCA)
- Weiterleitung von Abfragen an das Dokumentenregister und Ergebnisse vom Dokumentenregister zurückgeben
- Zugriffe werden protokolliert (ATNA)
- Bei Verwendung von XCA sind die Anforderungen und Empfehlungen aus Abschnitt 18.4.2 des IHE XCA Supplements umzusetzen.

Benötigte Schweizer Ergänzungen

- Richtlinien für die Bildung einer Community (gegebenenfalls aus bestehenden Communities) müssen definiert werden.
- Für einen domänenübergreifenden Datenaustausch müssen rechtliche Grundlagen geschaffen werden.
- Für XDS-Metadaten inkl. Dokumenttypen und -formate (classCode, formatCode) sollte ein CH-Standard entwickelt werden (vgl. auch Arbeiten zu Metadaten).
- Der Zugriff muss durch Policies (Richtlinien) geregelt werden. Ein Berechtigungssystem kontrolliert den Zugriff.
- Eine Community muss bei einem OID-Register registriert werden, um eine weltweit eindeutige ID zu erhalten (homeCommunityId).
- Richtlinien, wie mit lokalen IDs (z.B. Patienten-IDs, Behandelnden-IDs) in Metadaten umgegangen werden soll

Fazit

XCA erscheint aus unserer Sicht gut geeignet, über Community-Grenzen hinweg Daten auszutauschen. Da wenige Transaktionen unterstützt werden müssen, scheint dies ein interessanter Weg zu sein, auch nicht IHE Communities an die IHE Welt anzubinden. XDS.b und XCA können auch innerhalb einer Community zum Datenaustausch zwischen XDS Affinity Domains benutzt werden (z.B. Spitäler mit eigenen XDS Affinity Domains).

8.2 Reifegradstufen

Im Folgenden ein Vorschlag für die Reifegradstufen Dokumentenregister.

Stufe		Mindestanforderungen
A1	übergreifendes Element	Internationale Standards für Dokumenttype, -formate, -inhalte und Metadaten
A2	übergreifend interoperabel	Gateway der Community implementiert XCA alle Communities ans Netzwerk angebunden
B1	lokal integriert, standardisiert	CH-Standards für Dokumenttype, -formate, -inhalte und Metadaten
B2	lokal integriert, lokale Normen	Über das Profil XCA können Domänen (XDS Affinity Domains) so verbunden werden, dass die Suche nach einem Dokument mit Metadaten auch von einer anderen Domäne aus möglich ist.
C1	strukturiert, standardisiert	Dokumentenregister entspricht XDS.b Document Register
C2	strukturiert, lokal	Dokumente werden mit Metadaten registriert Dokumente können anhand von Metadaten gesucht werden
D1	elektronisch ad-hoc	Dokumente werden in elektronischer Form registriert
D2	nicht elektronisch	Dokumente werden in Papierform registriert (z.B. alphabetisch sortierte Patientendossiers)

Tabelle 19: Reifegradstufen Dokumentenregister

8.3 Szenarien / Abläufe

Dieses Unterkapitel diskutiert verschiedene Szenarien und Abläufe rund um Dokumentenregister.

Zugriff auf Dokumentenregister

Szenario: Zugriff aus eigener Domäne
- geregelt innerhalb der Domäne, es muss keine spezieller Use Case behandelt werden

Szenario: Zugriff aus eigener Community
- geregelt innerhalb der Community, es muss keine spezieller Use Case behandelt werden

Szenario: Zugriff von ausserhalb der eigenen Community
→ Siehe Use Case 10 (Kap. 3.3)

Zusammenführen von Communities

Falls mehrere Communities zusammengeführt werden müssen, gibt es verschiedene Varianten, wie dies umgesetzt werden könnte. Die nachfolgenden Varianten sind nicht abschliessend.

Variante 1: Fusion mit Migration der Dokumentenregister
Zusammenführen der beiden Dokumentenregister. Die Einträge werden in einem neuen Register erfasst, bzw. bei einem bestehenden Register zusammengefasst:

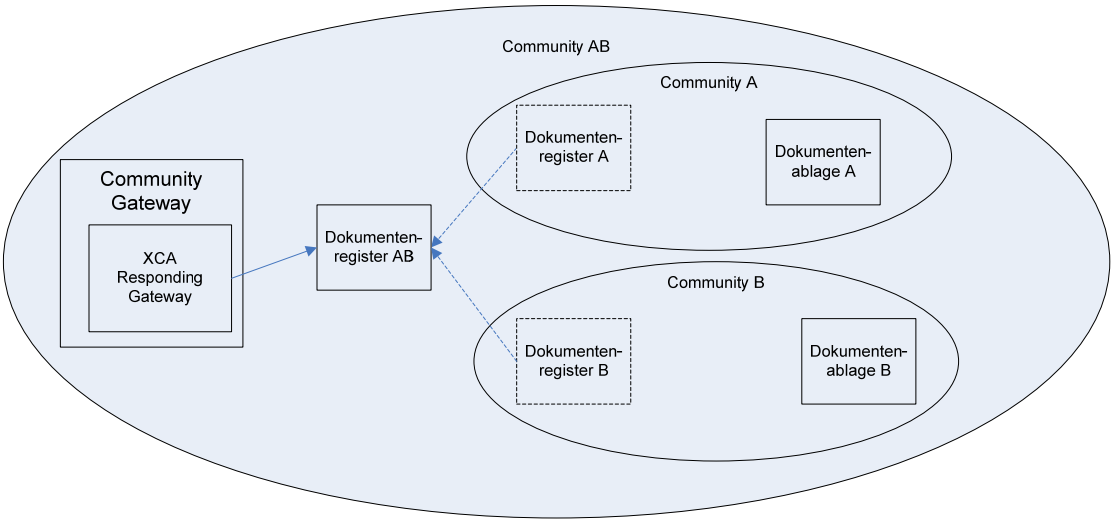


Abbildung 10: Ausgestaltung Fusion mit Migration der Dokumentenregister

Falls die XDS Affinity Domains die gleiche Patient Identifier Domain benutzen, müssen Patienten-IDs der Dokumentenregister nicht umgeschlüsselt werden.

Variante 2: Fusion mit XCA

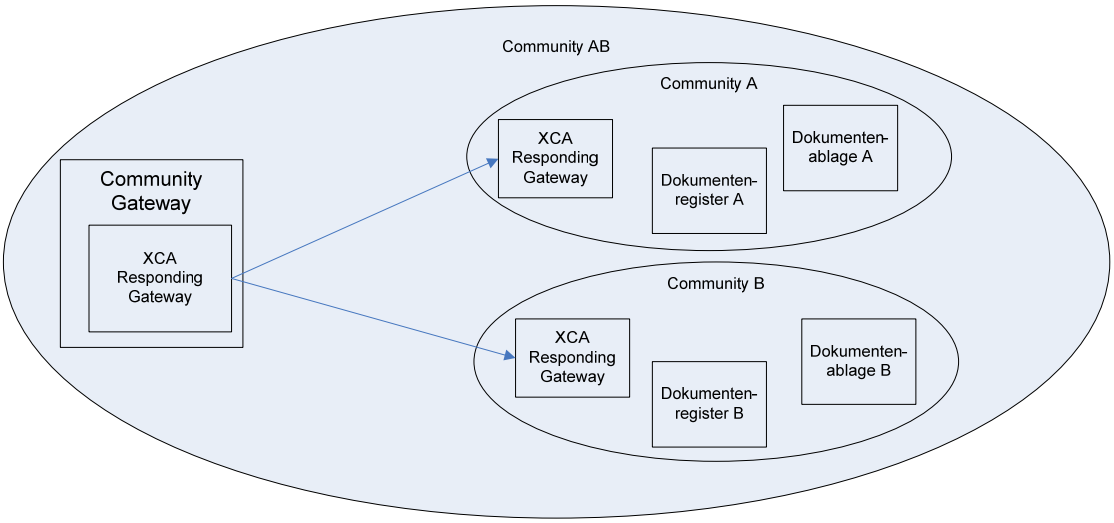


Abbildung 11: Ausgestaltung Fusion mit XCA

In diesem Beispiel bedient ein Responding Gateway (als Teil des Community-Gateways) zwei in dieser Community enthaltenen (Unter-)Communities. Diese beiden Communities müssen nicht unbedingt XDS Affinity Domains sein, da sie für den Initiating Gateway nicht sichtbar sind.

8.4 Nächste Schritte / offene Punkte

Titel	**Spezifikation der CH-spezifischen Umsetzung der Dokumentenregister**
Details	Für XDS-Metadaten inkl. Dokumenttypen und -formate (classCode, formatCode) sollte ein CH-Standard entwickelt werden. Wie wird mit sich ändernden Standards für die Metadaten umgegangen? (Historisierung der Metadatenstandards) Was soll mit Dokumenten passieren, dessen Metadaten nicht den vereinbarten Standards von eHealth-Schweiz entsprechen (z.B. weil sie vor der Existenz solcher Standards erstellt wurden)? Beim Document Consumer können sie evtl. nicht richtig angezeigt werden. Richtlinien, wie mit lokalen IDs (z.B. Patienten-IDs, Behandelnden-IDs) in Metadaten umgegangen werden soll

9 Dokumentenablage

Eine Dokumentenablage speichert Dokumente auf transparente, sichere, zuverlässige und dauerhafte Weise und beantwortet Abfragen von Dokumenten [ITI TF-1].

9.1 Architektur

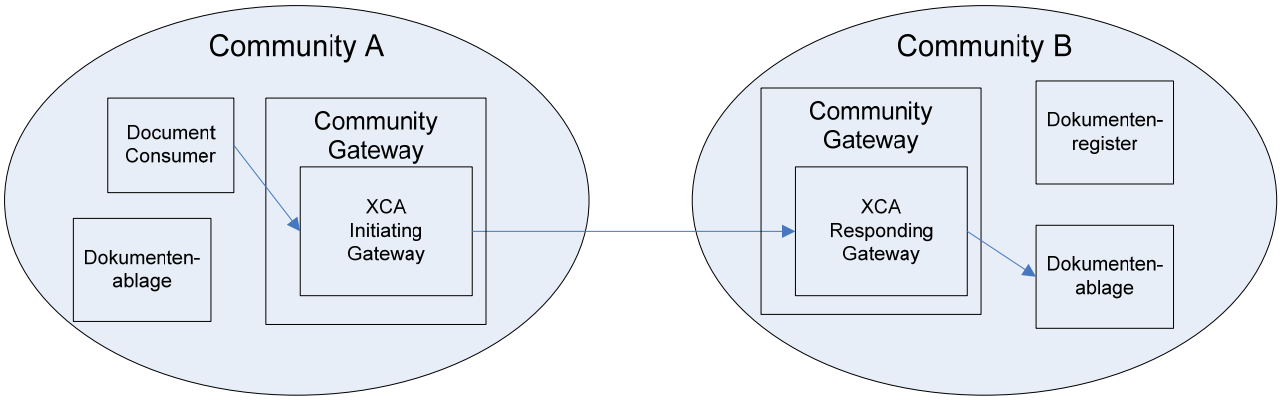


Abbildung 12 Cross-Community-Zugriff auf eine Dokumentenablage mit XCA

Anforderungen an eine Dokumentenablage

Aufgaben:
- Speichern von Dokumenten mit einer ID
- Abholen von Dokumenten mit einer ID
- Die Integrität der Daten wird sichergestellt.
- Die Dokumentenablage muss eine weltweit eindeutige ID aufweisen. Im Dokumentenregister wird diese ID in den Metadaten eines Dokuments referenziert.

Designprinzipien:
- Die Dokumenten-ID ist weltweit für immer eindeutig und an einen festen Dokumentinhalt gekoppelt.
- Der Inhalt des Dokuments spielt eigentlich keine Rolle. Dokumente werden genauso zurückgegeben, wie sie abgelegt wurden.
- Inhalte, Signatur, Verschlüsselung etc. von Dokumenten sollten in Richtlinien von eHealth Schweiz definiert werden.
- Der Zugriff auf die Dokumentenablage wird über das Berechtigungssystem kontrolliert.
- Andere Communities greifen über den XCA-Gateway auf die Dokumentenablage zu.

Funktionale Anforderungen für eine Dokumentenablage in einer XDS Affinity Domain:
- Eine Dokumentenablage wird durch den Actor Document Repository des IHE-Profils XDS.b realisiert.
  - Das Document Repository hat eine weltweit eindeutige OID (repositoryUniqueId).
  - Die Transaktionen ITI-41 Provide and Register Document Set-b, ITI-42 Register Document Set-b und ITI-43 Retrieve Document Set werden unterstützt.
  - Jedes abgelegte Dokument hat eine weltweit eindeutige ID (XDSDocumentEntry.uniqueId) [ITI TF-2b].
  - Das Document Repository ist an den XCA Actors Initiating Gateway und an den Responding Gateway angebunden.

– Das Document Repository lässt Erweiterungen bzgl. der Signatur oder Verschlüsselung von Daten zu (z.B. mit dem IHE-Profil DSG).

Anforderungen an den Gateway

Aufgaben:

- standardisierte Schnittstellen (XCA)
- Weiterleitung von Abfragen an die Dokumentenablage und Ergebnissen von der Dokumentenablage
- Zugriffe werden protokolliert (ATNA)
- Bei Verwendung von XCA sind die Anforderungen und Empfehlungen aus Abschnitt 18.4.2 des IHE XCA Supplements umzusetzen.

9.2 Reifegradstufen

Stufe		Mindestanforderungen
A1	übergreifendes Element	Dokumente sind unter einer weltweit eindeutigen ID abgelegt (bereits erfüllt mit XDS). Die Dokumentenablage hält sich an übergeordnete Standards.
A2	übergreifend interoperabel	Gateway einer Community implementiert XCA, alle Communities ans Netzwerk angebunden
B1	lokal integriert, standardisiert	Die Dokumentenablage entspricht Standards der übergeordneten Stufe (Metadaten, Sicherheitsanforderungen, …).
B2	lokal integriert, lokale Normen	Über das Profil XCA, eine IT-Infrastruktur und ein Berechtigungssystem können Communities so verbunden werden, dass ein kontrollierter Zugriff auf ein Dokument auch von einer anderen Community aus möglich ist.
C1	strukturiert, standardisiert	Die lokale Dokumentenablage wird mit dem Profil XDS.b innerhalb einer XDS Affinity Domain durch Document Repositories realisiert. Dokumente werden von einer Document Source innerhalb der Domäne in einem lokalen Document Repository abgelegt.
C2	strukturiert, lokal	Dokumente können mit einer ID gespeichert werden. Dokumente können mit einer ID abgeholt werden.
D1	elektronisch ad-hoc	Dokumente liegen in elektronischer Form vor.
D2	nicht elektronisch	Dokumente in Papierform

Tabelle 20: Reifegradstufen Dokumentenablage

9.3 Szenarien / Abläufe

Die Dokumentenablage sollte immer zusammen mit dem Dokumentenregister betrachtet werden.

- Dokument ablegen (siehe Use Case 10 bzw. IHE-Transaktion ITI-41)
- Dokument ändern (nicht vorgesehen – neues Dokument mit neuer ID)
- Dokument abfragen (siehe Use Case 10 bzw. IHE-Transaktion ITI-43)

Szenario: Zugriff aus eigener Domäne
- geregelt innerhalb der Domäne, es muss kein spezieller Use Case behandelt werden

Szenario: Zugriff aus eigener Community
- geregelt innerhalb der Community, es muss kein spezieller Use Case behandelt werden

Szenario: Zugriff von ausserhalb der eigenen Community
→ Siehe Use Case 10 (Kap. 3.3)

Die Funktion der Dokumentenablage ist unabhängig vom Dokumenteninhalt, d.h. Signatur / Verschlüsselung von Dokumenten sollte auf einer anderen Ebene behandelt werden (z.B. von Document Source/Consumer).

Eine Volltextsuche in Dokumenten ist nicht Aufgabe der Dokumentenablage.

Wenn bereits auf lokaler Ebene weltweit eindeutige IDs (z.B. UUID) benutzt werden, kann diese ID auf allen Reifegradstufen beibehalten werden.

9.4 Nächste Schritte / offene Punkte

Keine

10 Zugang

Abgrenzung:
Gemäss Absprache mit dem Koordinationsorgan eHealth Bund-Kantone enthält dieses Kapitel nur Hinweise und Abgrenzungen.

Die Themenbereiche „Zugangsportal für Patienten und Bevölkerung“ sowie die „Administrativen und medizinischen Prozesse“ weisen ähnliche Fragestellungen auf. Deshalb werden diese beiden Punkte in einem gemeinsamen Kapitel „Zugang“ behandelt.
Administrative Anspruchsgruppen stellen einen weiteren Teilnehmerkreis mit speziellen Rechten dar, welcher durch eine entsprechende Erweiterung der Rollen im Rollenkonzept Berücksichtigung finden kann.

10.1 Architektur

Die folgende Abbildung illustriert die generische Architektur für den Zugang

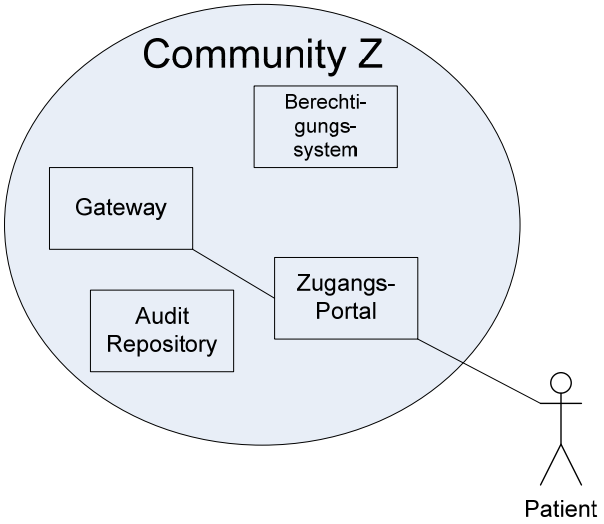


Abbildung 13: Generische Architektur für den Zugang (illustriert am Zugangsportal für Patienten)

Szenarien

Die folgenden Szenarien sind denkbar:
- Zugang durch Patient
- Zugang durch weitere Personen (z.B. Vertrauenspersonen des Patienten)
- Zugang durch Behandelnde
  - in Anwesenheit des Patienten
  - in Abwesenheit des Patienten
  - mit expliziter Einwilligung des Patienten
  - in Notfallsituationen
- Zugang durch weitere Beteiligten für weitere Anwendungsfälle (zu definieren)

Je nach Szenario kann es sich beim Portal um ein Zugangsportal zum ePatientendossier oder um einen allgemeinen Zugang zum System eHealth Schweiz handeln.

Ausgestaltung

Für all diese Szenarien sind die detaillierten Aufgaben prinzipiell gleich (vor dem Hintergrund der definierten und durch das Berechtigungssystem durchgesetzten Berechtigungen):

- Lesender Zugriff aus das persönliche Patientendossier
- Verwalten von Zugriffsrechten auf das Dossier (Wer hat Zugriff?)
- Abfragen und quittieren von Audit-Messages zur Verifikation ob ein Zugriff gerechtfertigterweise erfolgt ist (allenfalls mit Unterstützung des Hausarztes)
- Hinzufügen von Informationen

Design-Prinzipien:

- Ausgestaltung im Rahmen des Community-Konzeptes mit Gateways, Audit Repository und Berechtigungssystem.
- Je nach Szenario müssen zusätzliche Rollen definiert werden.
- Sollten weitere Daten hinzugefügt werden, so sind diese von Daten im medizinischen Kontext strikt zu trennen.
- Von der Technologiearchitektur her für mögliche Anbieter zahlreiche Varianten denkbar.
- An die organisatorische Ausgestaltung sind entsprechende Anforderungen zu definieren und zu überprüfen.

10.2 Nächste Schritte / Offene Punkte

Titel	**Konkretisierung Szenarien Zugang (fachlich/technisch)**
Details	Welche Anspruchsgruppen des Gesundheitssystems sollen auf welche Art und Weise am Gesamtsystem teilhaben / Zugang erlangen? Wie sieht die technische Referenzarchitektur für einen solchen Zugang genau aus?

Titel	**Erweiterung Rollenkonzept um weiteren Teilnehmerkreis**
Details	Weitere strukturelle Rollen (z.B. aus den Bereichen Forschung, Pharma, Versicherungen, Regulator etc.) Weitere funktionale Rollen (z.B. „mein Versicherer“)

11 Referenzen und Glossar

11.1 Referenzen

[EGov-ModellCSP]	Konzept eines homogenen Berechnungsmodells zur Ermittlung des qualitativen Nutzens und der Wirtschaftlichkeit von E-Government-Vorhaben, Wettbewerbsbeitrag von CSP, veröffentlicht durch das ISB
[epSOS-IM]	Identity Management in eHealth based on epSOS, epSOS Project, 2009 http://www.epractice.eu/files/EC%20epSOS%20Presentation.pdf
[ITI TF-1]	IHE IT Infrastructure Technical Framework – Volume 1 “Integration Profiles”, Revision 6.0 – Final Text, 10.08.2009.
[ITI TF-2b]	IHE IT Infrastructure Technical Framework – Volume 2 “Transactions Part B”, Revision 6.0 – Final Text, 10.08.2009.
[ITI TF-XCA]	IHE IT Infrastructure Technical Framework – Supplement 2009-2010 “Cross-Community Access”, Trial Implementation Supplement, 10.08.2009.
[ITI WP-CrossCommunityInfoExchange]	IHE IT Infrastructure Technical Framework White Paper “Cross Community Information Exchange including Federation of XDS Affinity Domains, Version 3.3, 10.10.2008
[ITI_WP-AccessControl]	IHE IT Infrastructure White Paper “Access Control”, 28.09.2009, IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
[ITI-VocRegDataDict]	ITI Vocabulary Registry and Data Dictionary http://wiki.ihe.net/index.php?title=ITI_Vocabulary_Registry_and_Data_Dictionary
[MEDNET-TS-001]	MEDNET NHIN Gateway – MEDNET Technical Specification, 2009.
[OID Konzept]	OID Konzept für das Schweizerische Gesundheitswesen – Zur Umsetzung der Strategie "eHealth" Schweiz, Stand: Version 1.1 vom 07. Dezember 20
[Rand2008IdentityCrisis]	Identity Crisis, An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System, RAND Health, 2008. http://www.rand.org/pubs/monographs/MG753/
[Rollenkonzept]	Rollenkonzept, Version 1.0 vom 28.03.2010 Noch nicht veröffentlicht. Weitere Informationen über info@e-health-suisse.ch erhältlich.
[UkSaferPracticeNotice]	Risk to patient safety of not using the NHS Number as the national identifier for all patients, National Patient Safety Agency, 2009 http://www.nrls.npsa.nhs.uk/resources/?entryid45=61913
[UseCaseDokument]	Gemeinsame Use cases für die prioritären Lieferobjekte aus der Umsetzung der eHealth Strategie Schweiz. Version 1.0 vom 12.02.2010. Noch nicht veröffentlicht. Weitere Informationen über info@e-health-suisse.ch erhältlich.

11.2 Glossar

Dieses Unterkapitel definiert verschiedene wichtige Begriffe. Wo möglich wurde auf Definitionen des eHealth Glossar des Koordinationsorgans Bund-Kanton zurückgegriffen (http://www.e-health-suisse.ch/glossar/index.html).

Begriff	**Beschreibung**
ATNA	Audit Trail and Node Authentication
Authentifizierung	Authentifizierung ist der Vorgang der Überprüfung einer behaupteten Identität.
Backbone	Ein verbindender Kernbereich eines übergreifenden Kommunikationsnetzes. Es kann sich dabei um reine Kommunikation aber auch um weitergehende Applikationsfunktionalität handeln.
Berechtigungssystem	Konzept, welches für die verschiedenen Benutzergruppen eines Informatikgefässes mittels definierter Rollen festlegt, welche Datenbereiche diese einsehen und/oder bearbeiten dürfen.
Community	Allgemeine Definition: Gruppe von Organisationen/Systemen, welche im Gesundheitsbereich tätig sind und auf Grund gewisser Gemeinsamkeiten (örtlich / inhaltlich / rechtlich) zusammenarbeiten. Definition gemäss IHE: A community is defined as a group of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing health information via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc. A community is identifiable by a globally unique id called the homeCommunityId.
Community Gateway	Synonym mit → „Gateway“ der Community
CT	Consistent Time: dieses IHE Profil stellt sicher, eine gemeinsame, übergreifenden konsistent Zeit verwenden.
ePatientendossier	Das elektronische Patientendossier ist die fortschreibbare Sammlung der verfügbaren persönlichen medizinischen, präventiven, pflegerischen und administrativen Daten. Unter anderem enthält das elektronische Patientendossier die individuelle Krankengeschichte, wichtige Laborbefunde, Operationsberichte sowie Röntgenbilder und digitale Daten anderer Untersuchungen. Das ePatientendossier wird von den Behandelnden in Absprache mit den Patientinnen und Patienten geführt. Die Inhalte stehen entlang des Behandlungspfades unabhängig von Ort und Zeit zur Verfügung.
epSOS	epSOS ist ein europäisches eHealth-Projekt, welches in einem ersten Schritt auf „Patient Summary“ / Notfalldaten fokussiert. Siehe http://www.epsos.eu/
FDS	Federated Directory Services: ein in Entstehung befindliches Profil; es umfasst verschiedene andere Profilanträge wie z.B. das HPD Profil („Healthcare Provider Directory“), welches ein Verzeichnis sowohl für Behandelnde als auch für Gesundheitsinstitutionen definiert.
Gateway	„Eingangspforten“ / „Netzübergänge“, welche die Communities an das Gesamtsystem eHealth Schweiz anbinden und so die übergreifende Zusammenarbeit ermöglichen.
Gesamtsystem eHealth Schweiz	Gesamtheit aller Systeme / Organisationen, welche an der Umsetzung der Strategie „eHealth“ Schweiz teilnehmen.
GLN	Global Location Number. Sie identifiziert international die volle Unternehmens- oder Betriebsbezeichnung sowie die Anschrift.
Health Data Locator	Health Data Locator is a function provided by a community or external entity that manages the locations of patient health data for a selected set of patients. A Health Data Locator keeps track of communities that know a patient and provides a list of these communities to a requesting community.

	(IHE Glossar vom XCPD Supplement)
HPI	Health Professional Index in Australien: Healthcare Provider Identifier (siehe auch HPI-I und HPI-O)
HPI-Dienst	Ein zentraler Verzeichnisdienst, der auf Anfrage durch berechtigte Systeme für Behandelnde, welche am System eHealth Schweiz teilnehmen, gewisse definierte vertrauenswürdige Attribute/Merkmale bereitstellt. Führende Systeme für die Behandelnden und ihre Attribute/Merkmale sind die sog. → „sektoriellen HPI“
HPI-I	Healthcare Provider Identifiers – Individual (ein Begriff aus der Ausgestaltung in Australien, siehe Kap. 7.1.4)
HPI-O	Healthcare Provider Identifiers – Organisation (ein Begriff aus der Ausgestaltung in Australien, siehe Kap. 7.1.4)
ID	Identifikator: ein eindeutiges künstliches Merkmal, das zur Identifizierung eines Objektes dient. Identifikatoren bestehen in der Regel aus Codes und Nummern. Auch Menschen können einen Identifikator erhalten (Personenidentifikator).
Identifikation	Die Identifikation ist der Vorgang, der zum eindeutigen Erkennen einer Person oder eines Objektes dient. In der Informationstechnologie bedeutet sie die Erkennung eines Benutzers (oder eines Administrators).
IHE	Integrating the Healthcare Enterprise: Initiative von Anwendern und Herstellern mit dem Ziel, den Informationsaustausch zwischen IT-Systemen im Gesundheitswesen zu standardisieren und zu harmonisieren
lokaler HPI	“Lokale” Behandelndenverzeichnisse, welche spezifische / lokale Attribute / Merkmale von Behandelnden verwalten und typischerweise Teil des lokalen Identity and Access Managements (IAM) sind.
MedReg	Gesundheits-/Medizinalberuferegister, welches das BAG im Rahmen des MedBG aufgebaut hat und unter www.medreg.admin.ch der Öffentlichkeit zur Verfügung stellt.
Meta Community	Eine hierarchische Gruppierung von Communities zu einer neuen Community [ITI WP-Cross¬Community¬Info¬Exchange]
National Contact Point	Der National Contact Point ist eine spezielle Community, welche den eigentlichen NCP gemäss epSOS enthält und so die Schweiz an die europäische (epSOS-)Infrastruktur anbindet.
NCP	National Contact Point (gemäss epSOS)
OID	Object Identifier: weltweit eindeutige Objekt Identifikationen
Patient Identifier Cross-reference Domain	Consists of a set of Patient Identifier Domains known and managed by a Patient Identifier Cross-reference Manager Actor. The Patient Identifier Cross-reference Manager Actor is responsible for providing lists of “alias” identifiers from different Patient Identifier Domains.
Patient Identifier Domain	A single system or a set of interconnected systems that all share a common identification scheme for patients.
Registry	Verzeichnis
sektorieller HPI	Dezentrale Verzeichnisse (z.B. von Berufsverbänden), welche die vertrauenswürdigen Personendaten halten, welche durch den zentralen HPI-Dienst abfragbar sind.
TLS	Transport Layer Security: ein Verschlüsselungsprotokoll zur sicheren Datenübertragung in öffentlichen Netzwerken.
XDS	“Cross Enterprise Document Sharing” ein Profil von IHE, welches den Austausch von medizinischen Dokumenten zwischen Einrichtungen ermöglicht.
XDS Affinity Domain	A group of healthcare enterprises that have agreed to work together using a common set of policies and which share a common infrastructure of repositories and a registry.