Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Standards und Architektur Empfehlungen III

Personenidentifikation und Berechtigungssystem

Verabschiedet vom Steuerungsausschuss

Bern, 27. Oktober 2011

ehealthsuisse
Koordinationsorgan Bund-Kantone
Organe de coordination Confédération-cantons
Organo di coordinamento Confederazione-Cantoni

Impressum

Projektorganisation:

Steuerungsausschuss: Didier Burkhalter (Bundesrat, Vorsteher EDI, Vorsitz), Pascal Strupler (Direktor BAG), Stefan Spycher (Vizedirektor BAG), Andreas Faller (Vizedirektor BAG), Carlo Conti (Regierungsrat, Vorsteher GD BS), Guido Graf (Regierungsrat, Vorsteher GD LU), Heidi Hanselmann (Regierungsrätin, Vorsteherin GD SG), Pierre-François Unger (Regierungsrat, Vorsteher GD GE)

Projektleitungsgremium: Adrian Schmid (Geschäftsstelle eHealth Bund-Kantone, Vorsitz), Christian Affolter (santésuisse), Lotte Arnold (SPO), Salome von Greyerz (BAG), Hansjörg Looser (GD SG), Caroline Piana (H+), Georg Schielke (GDK), Michael Stettler (BAG), Walter Stüdeli (IG eHealth), Judith Wagner (FMH), ,

Mitglieder „Teilprojekt Standards und Architektur": Hansjörg Looser (Kanton SG / Co-Leitung), Christian Lovis (H+ / Co-Leitung), Judith Wagner (FMH / Co-Leitung), Jürg Aeschlimann (BAG), Annalies Baumann (SVBG), Pierre-Yves Baumann (EDÖB), Susanna Bürki Sabbioni (SVBG), Patrick Caron (OFAC), Marco Demarmels (eCH), Anders Elleby (IG eHealth), Salome von Greyerz (BAG), Dominik Hadorn (Spitex Schweiz), Sang-Il Kim (IG eHealth), Birgit Lang (Suva), Thomas Lanz (Suva), Jean-Marie Leclerc (Kanton GE), Reto Mettler (VSFM), Willy Müller (ISB), Henning Müller (Fachhochschule Westschweiz), Maja Mylaeus (Spitex Schweiz), Philipp Negele (IG eHealth), Marc Oertle (H+), Serge Reichlin (IG eHealth), Michel Roulet (TMI Consulting), Martin Rüfenacht (IG eHealth), Ulrich Schaefer (Refdata), Tony Schaller (HL7), Rolf Schmidiger (SUVA), Michael Schumacher (Fachhochschule Westschweiz), Burkhard Schwalm (EDÖB), Christian Studer (H+), Barbara Widmer (PRIVATIM), Omar Vanoni (Kanton TI), Daniel Voellmy (H+), David Voltz (pharmaSuisse), Urs Zellweger (santésuisse),

Geschäftsstelle eHealth Bund-Kantone: Adrian Schmid (Leitung), Catherine Marik, Stefan Wyss, Isabelle Hofmänner.

Fachliche Beratung: Christian Lovis (Hôpitaux Universitaires de Genève HUG, Präsident SGMI)

Weitere Informationen und Bezugsquelle:
www.e-health-suisse.ch

Zweck und Positionierung dieses Dokuments

Der Steuerungsausschuss von Bund und Kantonen zur Umsetzung der „Strategie eHealth Schweiz“ hat am 20. August 2009 und am 20. Oktober 2010 in diversen Themen Empfehlungen verabschiedet. Zudem wurde am 27. Januar 2011 das Evaluationskonzept Modellversuche verabschiedet. Das vorliegende Dokument enthält Vorschläge für weitere Empfehlungen im Bereich von „Standards und Architektur“. Als Vorbereitung dienten zwei Inputarbeiten des Firmenkonsortiums Post/ELCA/Abraxas (Berechtigungskonzept) und der Firma keyon in Zusammenarbeit mit Urs Bürge Beratungen GmbH (Personenidentifikation). Die Empfehlungsdokumente und die Vorbereitungsarbeiten sind zugänglich unter www.e-health-suisse.ch.

Im Interesse einer besseren Lesbarkeit wurde auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

Inhaltsverzeichnis

1 Ausgangslage

1.1 Einleitung

Bisherige Empfehlungen als Basis

Grundlage dieses Dokumentes sind die bisherigen Empfehlungen und Berichte von "eHealth Suisse" (siehe www.e-ehealth-suisse.ch). Zudem beantwortet das vorliegende Dokument Fragen zum Thema der eindeutigen Personenidentifikation als Grundvoraussetzung für das Bereitstellen und Abrufen von Daten, derer Stellenwert in den Empfehlungen I des Teilprojektes Standards und Architektur vom 19. März 2009 unterstrichen wurde (Seite 6).

Positionierung des vorliegenden Dokumentes

Das vorliegende Dokument beschreibt auf fachlicher Ebene, wie die Personenidentifikation und das Berechtigungssystem ausgestaltet sein sollen. Zum Teil definiert das Dokument neue Aufgaben, deren Zuständigkeit noch offen ist. Diese Zuständigkeit sowie die der Verbindlichkeit bei der Anwendung sind politische Entscheide, die im Rahmen der Rechtsetzungsprojekte geklärt werden müssen. Denkbar sind rechtliche Grundlagen auf Bundes- oder Kantonsebene – oder vertragliche Vereinbarungen zwischen den Akteuren.

Bedeutung der Identifikation von Personen und einheitlicher Zugriffsregeln

Eine verlässliche Identifikation von Patienten und Behandelnden sowie klare Regelungen für den Zugriff auf medizinische Daten schaffen für alle beteiligten Akteure einen sicheren Vertrauensraum ("trusted domain") in dem Daten problemorientiert und nutzbringend bereitgestellt und abgerufen werden können. Auch im Rahmen der europäischen Koordination wird die Bedeutung der Themen unterstrichen. Dies mit folgenden Argumenten:

- Eine verlässliche und vertrauenswürdige Identifizierung und Authentisierung der beteiligten Akteure (speziell von Patienten und Behandelnden) ist notwendig, damit die rechtlichen Anforderungen des Datenschutzes und der Datensicherheit erfüllt werden können;
- Eine zuverlässige Identifizierung und Authentisierung ist eine notwendige Bedingung, dass sich das Vertrauen in die Sicherheit von „eHealth“-Anwendungen entwickeln kann. Nur so ist jene Akzeptanz bei den Patienten und Behandelnden zu gewinnen, die zu einer breiten Nutzung von „eHealth“-Anwendungen führt;
- Patienten und Behandelnde müssen sicher identifiziert und authentisiert werden können, damit die richtigen Informationen zur richtigen Person zur richtigen Zeit zur Verfügung stehen;
- Mit einem Berechtigungssystem wird abgesichert, dass nur berechtigte Personen Zugriff auf die Daten haben.

Datensicherheit

Der Zugriff auf die Daten und die Datenübertragung werden angemessen geschützt. Die in den Empfehlungen II des Teilprojektes Standards und Architektur vom 21. Oktober 2010 empfohlenen IHE-Profile bedingen eine konsequente Datenverschlüsselung.

Die in der Folge empfohlenen Konzepte beziehen sich in der „Architektur eHealth Schweiz“ auf die drei schweizweit koordinierten Komponenten „Identifikation Bevölkerung / Patienten“, „Identifikation Behandelnde“ und „Berechtigungssystem (siehe Grafik).

Drei schweizweit koordinierte Komponenten

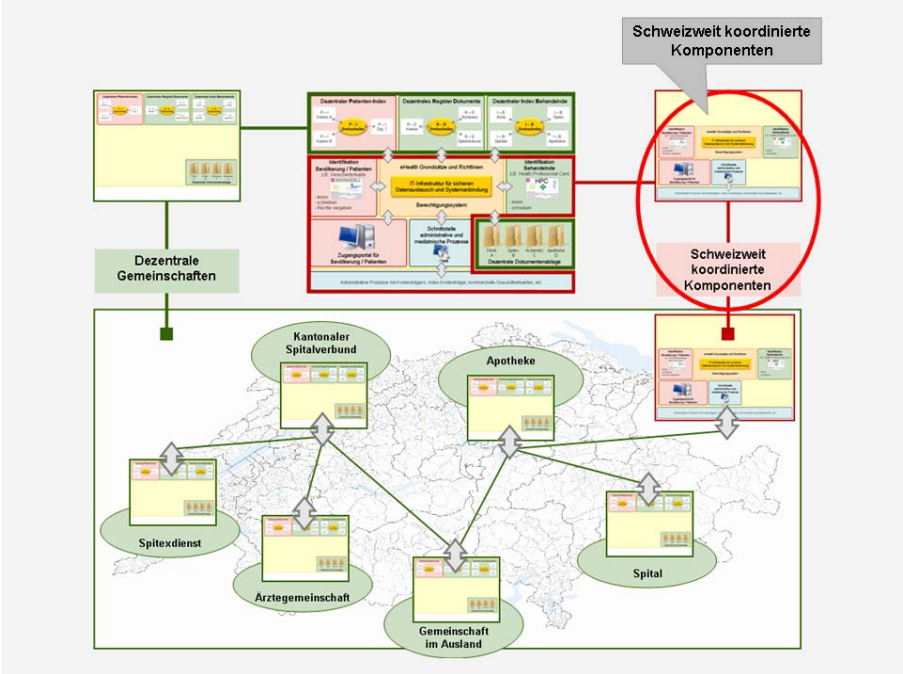


Abbildung 1: Positionierung in der „Architektur eHealth Schweiz“

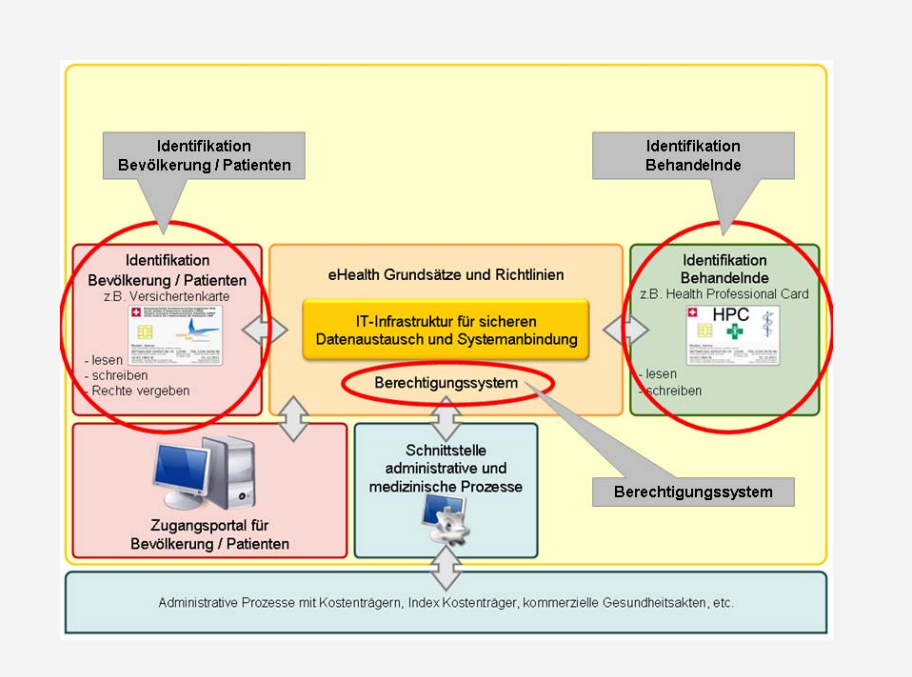


Abbildung 2: Drei der schweizweit koordinierten Komponenten

Bereitstellen und Abrufen von Daten zwischen Gemeinschaften

Gemäss den Empfehlungen II des Teilprojektes Standards und Architektur vom 21. Oktober 2010 ist eine Gemeinschaft eine organisatorische Einheit von Behandelnden, die

- an der Patientenbehandlung beteiligt ist und
- patientenbezogene Informationen erstellt oder verwendet und
- patientenbezogene Informationen für andere Gemeinschaften bereitstellt oder von anderen Gemeinschaften abruft.

Die folgenden Empfehlungen beziehen sich auf das Bereitstellen und Abrufen von Daten zwischen Gemeinschaften und nicht innerhalb einer Gemeinschaft.

HPI-Dienst

Für das Bereitstellen und Abrufen von Daten ist auch ein schweizweiter „Health Professional Index Dienst (HPI-Dienst) notwendig (siehe Empfehlungen II „Standards und Architektur“ vom 21. Oktober 2010, Seite 15). Ein HPI-Dienst überprüft und bestätigt verlässlich die Zugehörigkeit von Behandelnden zu den jeweiligen Berufsgruppen. Er ist nicht Gegenstand der vorliegenden Empfehlungen.

1.2 Begriffe

Identifizierung

Die Identifizierung ist ein Vorgang, der zum eindeutigen Erkennen einer Person oder eines Objektes dient.[1] Sollen Computersysteme Objekte bzw. Personen erkennen, werden – weil das direkt meist nicht möglich oder zu aufwändig ist – Identifikatoren verwendet. Ein Identifikator ist ein künstlich zugewiesenes Merkmal zur eindeutigen Identifizierung einer Person oder eines Objektes.[2] (Beispielsweise verweist eine Hausnummer als Identifikator innerhalb einer Strasse auf ein bestimmtes Haus.) Als Identifikatoren werden häufig Kennzahlen oder „Codes“, d.h. Kombinationen aus Nummern und/oder Buchstaben verwendet.

Identität

Unter Identität wird häufig die Kombination der Merkmale verstanden, anhand derer sich ein Individuum von anderen unterscheiden lässt: Das erlaubt eine eindeutige Identifizierung. Bei einer Person sind dies zum Beispiel Merkmale wie Name, Vorname, Geschlecht, Geburtsdatum, Wohnort, biometrische Daten oder Kennzahlen. Eine „Einheit“ (Entität) kann alles sein, was eindeutig als solche erkannt werden kann (Person, Gerät, Objekt, Gruppe, Organisation, etc.). Einheiten können mehrere Identitäten haben, die in verschiedenen Kontexten verwendet werden können.

Digitale Identität

Unter dem Begriff der „Digitalen Identität“ wird eine Kombination von Attributen einer Person in elektronischer Form verstanden. Die digitale Identität kann wechseln, und eine Person kann auch mehrere digitale Identitäten haben.

Im Kontext des „Digitalen Identitätsmanagements“ sind folgende Themen relevant:

- Geltungsbereich (innerhalb von Organisationen oder organisationsübergreifend);
- Lebenszyklus der Identität: Einrichten, verändern, entziehen, beenden, archivieren;
- Verwalten und Schützen der Informationen (Attribute) der Identität, die sich über die Zeit ändern;
- Zuweisen und Verwalten der verschiedenen Rollen von Identitäten;
- Verknüpfen der Rollen mit Pflichten, Verantwortungen, Privilegien und Rechten für den Zugriff auf Ressourcen;
- Systeme, in denen die Daten gespeichert werden (Verzeichnisse, Datenbanken, etc.);
- Medien als Träger von Identitäten (z.B. Token, Karten).

---

[1] Quelle: Wikipedia
[2] Quelle: Wikipedia

Identifizierung von Patienten

Im Gesundheitswesen kommt der Identifizierung von Patienten eine zentrale Bedeutung zu. Nicht nur Daten oder Dokumente müssen dem richtigen Patienten zugeordnet werden, sondern auch Proben oder Therapien. Im Rahmen der „Architektur eHealth Schweiz“ werden Patienten von den Behandelnden registriert und die Daten im Master-Patient-Index der Gemeinschaft verfügbar gemacht. Analog zur Identifikation von Patienten müssen auch Dokumente, die einem Patienten zugeordnet werden können, identifiziert werden. Dies geschieht durch die Zuweisung von Metadaten zu einem Dokument (z.B. Identifikatoren, Titel, Autor, Datum, Version).

Authentifizierung und Authentisierung

Authentifizierung ist aus Sicht eines Überprüfers der Nachweis (Verifizierung) der Echtheit einer behaupteten Eigenschaft einer Partei, die beispielsweise eine Person, ein Gerät, ein Dokument oder eine Information sein kann. Authentifizierung ist eine unmittelbare Folge der Authentisierung, welche die Sicht des Überprüften darstellt.

Durch den Vorgang der Authentisierung lässt sich die Rechtsgültigkeit einer Behauptung oder die eigene Identität nachweisen. Typischerweise authentisieren sich Personen gegenüber einem System und übergeben dabei ihre Authentisierungsmerkmale (über das Identifikationsmittel) zur Prüfung. Wer sich somit (aktiv) an einem System authentisiert, lässt sich (passiv) durch das System authentifizieren. Ist die Authentifizierung erfolgreich erfolgt, dann ist die Echtheit gegeben. Dies entspricht der Personen-Authentisierung, die Gegenstand dieses Dokuments ist.

Eine Authentisierung kann erfolgen durch:

- *Wissen:* Zum Beispiel durch Kenntnis eines Passwortes oder PIN:
- *Besitz eines Identifikationsmittel:* Zum Beispiel mit einer Smartcard, einem USB-Stick oder Schlüssel;
- *Biometrische Merkmale*: Zum Beispiel mit Fingerabdruck, Stimme oder Unterschrift in Anwesenheit des Benutzers.

Autorisierung

Erst die Autorisierung entscheidet, ob nach der Authentisierung und erfolgreicher Authentifizierung gewisse Dienste berechtigt in Anspruch genommen werden dürfen (Berechtigungssystem). Die Autorisierung bezeichnet insbesondere das Zuweisen und Überprüfen von Zugriffsrechten auf Daten und Dienste an Systemnutzer. Ein (häufiger) Spezialfall davon ist der erlaubte Zugriff auf sogenannte Ressourcen (z. B. auf Verzeichnisse oder Dateien) in einem Computernetzwerk.

Am Beispiel eines Bankgeschäftes authentisiert sich ein Kunde mit seiner Bankkarte (durch Besitz der Karte und durch Wissen der PIN) am Terminal. Das System authentifiziert ihn aufgrund der zwei Faktoren Besitz und Wissen als rechtmässigen Benutzer. Will er einen Geldbetrag von seinem Konto abheben, der aber die vorgegebene Limite übersteigt, wird der Vorgang abgebrochen, da keine Autorisierung durch die Bank vorliegt.

Auch ein einfaches System mit Name und Passwort (Wissen) kann zur Identifizierung und Authentisierung benutzt werden. Dabei behauptet der Benutzer seine Zugangsberechtigung, indem er einen Benutzernamen eingibt. Er au-

thentisiert sich, indem er sein Passwort angibt. Das Programm identifiziert den Benutzer anhand dieser Angaben und authentifiziert daraufhin dessen Zugangsberechtigung. Damit steht für das Programm die Echtheit des Kommunikationspartners fest. Dieses Verfahren gilt allerdings als schwach und wird in vielen Fällen als ungenügend erachtet..

Kombination ermöglicht die starke Authentisierung

Durch geeignete Kombination der Faktoren Wissen, Besitz und/oder biometrischer Merkmale kann eine starke Authentisierung erreicht werden. Die Stärke der Authentisierung definiert sich über den Ausgabeprozess der digitalen Identität. So kann z.B. eine SuisseID nur ausgestellt werden, wenn eine Überprüfung am Schalter mittels Pass oder Identitätskarte erfolgt ist. Ohne einheitlichen Ausgabeprozess hat ein Identifikationsmittel keinen Wert.

Identifikationsmittel

Ein Identifikationsmittel oder Security-Token (einfach: Token) ist eine Hardwarekomponente zur Identifizierung und Authentifizierung von Benutzern.

Stammgemeinschaft

Beim Eintritt ins System entscheidet sich der Patient für seine Stammgemeinschaft. Diese verwaltet alle aktuellen Einwilligungen und Zugriffsrechte eines Patienten (inklusive „„White- und Blacklist“ bzw. Ein- und Ausschlusslisten). Wenn eine Gemeinschaft bei den anderen Gemeinschaften eine Abfrage macht, dürfen die verfügbaren Dokumente erst angezeigt werden, wenn aus der Stammgemeinschaft bekannt ist, welche Einwilligungen und Zugriffsrechte der Patient erteilt hat. Mit dieser Information können Berechtigungen und Zugriffe durchgesetzt werden, denen der Patient zugestimmt hat. Die Eigenschaft „Stammgemeinschaft“ kann an eine andere Gemeinschaft übertragen werden (z.B. bei einem Umzug).

Daten und Dokumente

Beim Bereitstellen und Abrufen von Daten zwischen Gemeinschaften wird im Kontext der IHE Integrationsprofile von Dokumenten gesprochen. Unter einem "Dokument" wird generell ein Informationsobjekt verstanden, unabhängig der Anwendungsidee (z.B. Textdokument i.e.S., strukturierte Datensätze, Multimediadaten). Dokumente werden mittels Metadaten beschrieben und damit in der Basiskomponente "Dezentrales Register Dokumente" registriert. Mit dem Metadaten-Attribut 3.3 Datenformat (siehe Empfehlungen II des Teilprojektes Standards und Architektur vom 21. Oktober 2010, S. 23) wird das konkrete Datenformat des Dokumenteninhaltes beschrieben.

2 Personenidentifikation

Ziele der Identifikation von Personen

Damit die medizinischen Daten eines Patienten zusammengeführt werden können, ist eine eindeutige Identifikation sowohl der Patientinnen und Patienten als auch der Behandelnden notwendig. Dies mit den folgenden Zielen:

- *Vollständig:* Alle verfügbaren Dokumente werden zusammengeführt;
- *Eindeutig:* Die Dokumente werden dem richtigen Patienten zugewiesen;
- *Vertraulich:* Nur autorisierte (eindeutig identifizierte und berechtigte) Personen können auf die Dokumente zugreifen;
- *Nachvollziehbar:* Es kann nachvollzogen werden, wer welche Dokumente eingesehen oder bearbeitet hat.

Schwächen der heutigen Systeme

Bei einer steigenden Anzahl von Patienten und Gemeinschaften, die am System teilnehmen, kann mit Merkmalen wie Name, Vorname, Geburtsdatum etc. keine eindeutige Identifikation garantiert werden[3], Dies führt zu…

- … mehrdeutigen Resultaten;
- … falschen Zuteilungen von Dokumenten;
- … unvollständigen Dokumentationen;
- …aufwändigen manuellen Bereinigungen.

Notwendigkeit eines eindeutigen Identifikators

Elektronisches Bereitstellen und Abrufen von Daten bedingt eine eindeutige Identifikation der beteiligten Personen. Deshalb ist ein Identifikator notwendig,, der es erlaubt,

- eine digitale Identität der betreffenden Person zuzuweisen;
- festzustellen, dass eine von einer Person behauptete digitale Identität wahr ist;
- auf dieser Basis der Person Zugriffsrechte zuzuordnen.

Bezug zum Berechtigungssystem

Für den Aufbau und die Umsetzung eines Berechtigungssystems ist die eindeutige Identifikation von Personen aus folgenden Gründen notwendig:

- Personen müssen eindeutig identifiziert werden können (Patienten und Behandelnde);
- Dokumente (Objekte) müssen eindeutig identifiziert werden können;

[3] Die Fachliteratur berichtet von Fehlerquoten von bis zu 30% bei MPI-Lösungen, siehe z.B. Madison Information Technologies: Medical Record Number Errors: A Cost of Doing Business? o.O. 2001; Lenson, Celia M./Herr, Linda M: Preparing the Master Patient Index. For an Integrated Delivery System. In: Journal of AHIMA, November-December 1995, Vol. 66, No. 10, pp. 56-60 oder auch http://www.fortherecordmag.com/archives/062110p10.shtml

- Sind Patienten, Behandelnde und Dokumente eindeutig identifiziert, können Zugriffsrechte auf Dokumente vergeben werden (Berechtigungssystem).

So erhält eine Person eine digitale Identität

Schritte der Entstehung einer digitalen Identität sind:

- *Die Identität wird festgestellt (Erst-Identifikation):* Eine Person (Entität) wird anhand von bestimmten Eigenschaften (Attributen) von der zuständigen Instanz als eine bestimmte Person identifiziert. Es wird beispielsweise bei der Aufnahme eines Patienten in einer Gemeinschaft eine Reihe administrativer Daten erfasst (Name, Vorname, Geschlecht, Geburtsdatum, Wohnadresse, etc.);
- *Die digitale Identität wird definiert*: Eine Teilmenge der Attribute wird von der zuständigen Instanz ergänzt durch spezifische Attribute, die für eine digitale Identität notwendig sind (z.B. Identifikationsnummer);
- *Das Mittel der Identifikation wird erstellt:* Die Daten der digitalen Identität werden auf einen Träger aufgebracht (Identifikationsmittel). Möglich sind verschiedene Medien wie eine Versichertenkarte (VK), ein Signatur-Token wie die SuisseID, oder ein anderes System.

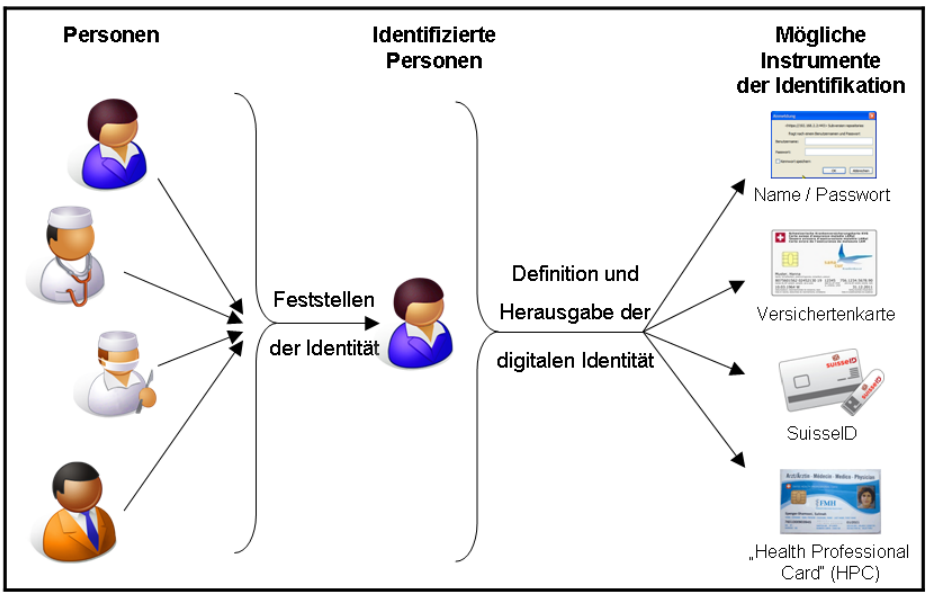


Abbildung 3: So entsteht eine digitale Identität

Verwendung einer digitalen Identität

Schritte bei der Verwendung einer digitalen Identität sind:

- *Identifikation und Authentisierung:* Der Besitzer des Identifikationsmittels weist sich mit dem Identifikationsmittel aus, wenn er auf das elektronische Patientendossier zugreifen will. Durch die Authentisierung und Authentifizierung wird überprüft, ob die behauptete Identität als gültig erachtet werden kann. Dabei wird eine Kennzahl (Personenidentifikator) verwendet, mit der die Person über das Identifikationsmittel verknüpft ist;

- *Mapping der digitalen Identität:* Da eine Person verschiedene Identifikationsmittel verwenden kann, soll die aus der Authentisierung resultierende Kennzahl (Personenidentifikator) in eine einheitliche Kennzahl abgebildet werden.

Identifikationsmerkmale für Patienten

Je verlässlicher die Identifikationsmerkmale, desto verlässlicher ist die Identifikation und damit das gesamte System. Die höchste Verlässlichkeit lässt sich mit einer schweizweit eindeutigen Kennzahl erreichen, die allen zu identifizierenden Personen zugeteilt wird und von den Berechtigten verwendet werden kann (z.B. AHVN13 oder eigene Kennzahl für das Gesundheitswesen).

Anforderungen an die Identifikation von Personen

Eine Person kann mehrere digitale Identitäten auf verschiedenen Trägern besitzen (Karten, USB-Sticks, etc.). Grundsätzlich sollen im Schweizer Gesundheitswesen unterschiedliche Möglichkeiten der Identifikation bestehen. Deshalb muss die Personenidentifikation so aufgebaut sein, dass…

- bestehende Identifikatoren verwendet werden können;
- die Verbindung zwischen digitaler Identität und Person frei verknüpft und wieder gelöst werden kann;
- verschiedene digitale Identitäten mit einem eindeutigen Identifikator verbunden werden können;
- zukünftige Systeme unterstützt werden können (Zusammenführen mit anderen Identifikatoren – zum Beispiel mit dem Konzept Identity- und Access-Management der E-Government-Strategie).

Bausteine der Identität einer Person

Vor diesem Hintergrund macht es Sinn, nicht allein auf eine schweizweit eindeutige Kennzahl zu setzen. Vielmehr sollte die Personenidentifikation aus verschiedenen Bausteinen zusammengestellt werden, die verknüpft und wieder gelöst werden können. Die Identität einer Person im Gesundheitswesen definiert sich aus folgenden Bausteinen:

- ① „Ich als Person“: Eigenschaften einer Person (Name, Vorname, Geburtsdatum, Geschlecht, etc.);
- ② „Meine digitale Identitäten“: Meine verschiedenen digitalen Identitäten (Name/Passwort, SuisseID, Versichertenkarte, HPC, etc.);
- ③ „Mein eindeutiger Identifikator“: Schweizweit eindeutige Kennzahl;
- ④ „Meine lokalen Identifikatoren“: Diverse Nummern, die in den Systemen der Behandelnden gebraucht werden und/oder auf Dokumenten stehen.

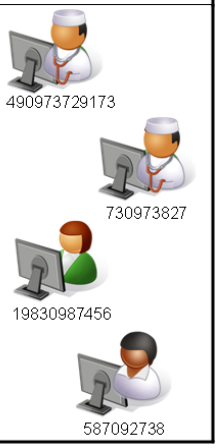
①	②	③	④
„Ich als Person“	**„Meine digitalen Identitäten“**	**„Mein eindeutiger Identifikator“**	**„Meine lokalen Identifikatoren“**
Name, Vorname, Geburtsdatum, Geschlecht etc.	Mittel und Träger der digitalen Identität	Schweizweit eindeutige Kennzahl	Kennzahlen in lokalen Anwendungen
 Patientinnen / Patienten  Behandelnde		**8338243438438384**	 490973729173 730973827 19830987456 587092738

Abbildung 4: Aufbau der Identität einer Person im Gesundheitswesen

Sinnvolle Kombination der Bausteine

Das Zusammenstellen der Patientenidentifikation mit diesen vier Bausteinen stellt sicher, dass mehrere digitale Identitäten verwendet werden können. Zudem werden Dokumente nicht mit der eindeutigen Kennzahl ③ referenziert, sondern wie bisher mit den lokalen Kennzahlen ④. Diese werden innerhalb einer Gemeinschaft im Master Patient Index (MPI) zu einer eindeutigen Kennzahl zusammengeführt. Diese stellt beim Bereitstellen von Daten für andere Gemeinschaften die Zuordnung der Dokumente zur richtigen Person sicher.

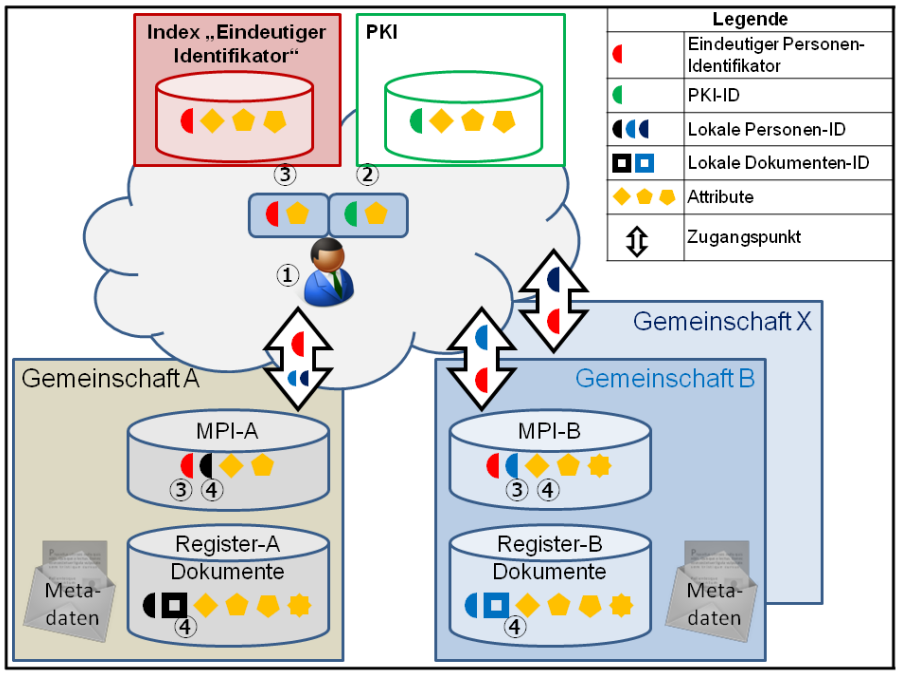


Abbildung 5: Die Personenidentifikation in und zwischen Gemeinschaften

Seite 14

Die Abbildung 5 stellt die kombinierte Anwendung der in Abbildung 4 bezeichneten Bausteine ①, ②, ③, ④ zur sicheren Personenidentifikation innerhalb und zwischen Gemeinschaften dar:

- Patienten ① die dem System «eHealth Schweiz» beitreten, erhalten über einen einheitlichen Ausgabeprozess sowohl ihre digitale Identität ② als auch einen eindeutigen Personenidentifikator ③. In der oben stehenden Abbildung 5 wird dafür z.B. der Index der eindeutigen Patientenidentifikation verwendet (roter Halbmond); von einer Public Key Infrastruktur (PKI) wird ein Zertifikat ausgestellt (z.B. auf einer Smartcard als Identifikationsmittel, grüner Halbmond)
- Der eindeutige Personenidentifikator ③ wird für die verlässliche Identifikation zwischen Gemeinschaften verwendet.
- Auf den dezentral gespeicherten, mit Metadaten beschriebenen Dokumenten und in den Dokumentenregistern der jeweiligen Gemeinschaften A, B und X werden ausschliesslich lokale Identifikatoren ④ verwendet („lokale Personen-ID“ als verschieden blaue Halbmonde und „lokale Dokumenten-ID“ als verschieden blaue Vierecke).
- In jeder Gemeinschaft stellt ein Master Patient Index (MPI-A, MPI-B, MPI-X) die logische Verbindung zwischen dem eindeutigen Personenidentifikator ③ und den verschiedenen lokalen Personen-ID ④ sicher. Dadurch können einerseits die in verschiedenen Quellen bereitgestellten Dokumente zu einem Patienten virtuell zusammengeführt werden. Andererseits wird ein schweizweit einheitlicher Personenidentifikator von den Dokumenten entkoppelt.
- Bei der Behandlung eines Patienten in Gemeinschaft A können durch Berechtigte alle freigegebenen Dokumente in A mittels lokaler Personen-ID (④ schwarzer Halbmond) gefunden werden. Für die Gemeinschaft übergreifende Suche sendet der Zugangspunkt den über dem MPI-A hergeleiteten eindeutigen Personenidentifikator ③ in Kombination mit anderen demographischen Attributen (gelb) an die Zugangspunkte der zertifizierten Gemeinschaften. Nur wenn der jeweilige MPI eine eindeutige Verknüpfung mit einer lokal registrierten Personen-ID (④ blaue Halbmonde) feststellen kann, sendet er die lokale Personen-ID als Antwort an den anfragenden Zugangspunkt. Die Abfrage der Dokumente erfolgt anschliessend direkt mit den jeweiligen lokalen Personen-ID und Dokumenten-ID.

Um eine eindeutige Identifikation von Personen zwischen Gemeinschaften zu erreichen, soll eine schweizweit eindeutige Kennzahl verwendet werden. Sie kann zusammen mit anderen Merkmalen für die Personenidentifikation zwischen Gemeinschaften verwendet werden. Dies gilt für Behandelnde und Patienten.	Empfehlung 1 Eindeutige Kennzahl für Personenidentifikation

Bevor Dokumente eines Patienten eingesehen werden dürfen, müssen sich Patienten und Behandelnde authentisieren. Authentifizierung bedeutet, mit einem akzeptablen Niveau an Sicherheit festzustellen, dass eine durch eine Person behauptete digitale Identität wahr ist.

Authentisierung und Authentifizierung

Die Stärke einer Authentisierung wird durch Anforderungen an das Identifikationsmittel, den Herausgabeprozess etc. bestimmt. Das Bundesgesetz über die elektronische Signatur (ZertEs) legt solche Anforderungen für die elektronische Signatur fest. Diese könnten für die Authentisierung übernommen werden. Vor der Umsetzung und Inbetriebnahme einer Authentisierungsmethode sollen die verschiedenen Vor- und Nachteile hinsichtlich Praktikabilität für den Benutzer im Alltag sorgfältig überprüft werden, damit das angestrebte Sicherheitsniveau tatsächlich erreicht werden kann. Patienten können zwischen den zugelassenen Identifikationsmitteln wählen.

Ausgabeprozess des Identifikationsmittels

Es ist eine starke Authentisierung durch eine geeignete Kombination von Wissen, Besitz und biometrischen Merkmalen anzuwenden.

Empfehlung 2

Authentisierung muss stark sein

3 Berechtigungssystem

Ziele des Berechtigungssystems

Alle im System «eHealth Schweiz» gespeicherten Daten und Dokumente betreffen konkrete Personen und sind besonders schützenswerte Personendaten. Um die Vertraulichkeit sicher zu stellen, sind verschiedene Massnahmen erforderlich. Hier wird nur der Aspekt Berechtigungskonzept beschrieben. Weitere Massnahmen wie z.B. Verschlüsselung werden zu einem späteren Zeitpunkt mit weiteren Empfehlungen beschrieben. Das Berechtigungssystem erlaubt es, dass der Patient als Eigentümer seiner Daten den Zugriff durch Dritte auf die eigenen Daten festlegen, durchsetzen und nachverfolgen kann. Dadurch steht der Patient im Zentrum und kann sein Recht auf informationelle Selbstbestimmung wahrnehmen.

Ziele des Berechtigungssystems sind:

- *Zugriff ermöglichen:* Allen Berechtigten stehen die zur Erfüllung der Aufgaben notwendigen Informationen zur Verfügung;
- *Vertraulichkeit gewährleisten:* Daten dürfen nur einsehbar sein, wenn die entsprechenden Berechtigungen vorliegen;
- *Zugriffe sinnvoll gestalten:* Grundlegende Voreinstellungen müssen allgemein verständlich und die Konsequenzen einer Änderung leicht erklärbar sein;
- *Transparenz und Vertrauen schaffen:* Das Berechtigungssystem muss in sich transparent sein und sämtliche Zugriffe nachvollziehbar darstellen. Dies schafft Vertrauen und ist eine wichtige Grundlage für die Akzeptanz des gesamten Systems.

Aufbau der Berechtigungsmatrix

Das Zugriffsberechtigungssystem regelt, wer (Subjekt) auf welche Ressourcen (Informationsobjekte) wie, wann und für wie lange zugreifen darf (Rechte). Für die Entscheidung, ob der Zugriff erteilt oder verweigert wird, müssen die einzelnen Einwilligungen, bzw. die festgelegten Regeln ausgewertet werden. Diese Regeln können aus der Kombination von Rollen und Vertraulichkeitsstufen in Form einer Berechtigungsmatrix aufgebaut werden.

Charakter des Systems

Es ist eine Grundcharakteristik des Systems, dass die betroffene Person solange uneingeschränkten Zugriff zu einem Dokument hat, wie sie die für eine Systemteilnahme erforderlichen Bedingungen erfüllt. In Ergänzung zu diesem Prinzip können persönliche Grundsätze des Zugriffs und individuelle Einwilligungen festgelegt werden. Metadaten werden hinsichtlich Zugriff gleich behandelt wie Dokumente.

Ein Patient kann seine Einwilligung zum ePatientendossier jederzeit und ohne Angabe von Gründen widerrufen. Es ist zudem denkbar, dass ein Dossier Dokumente enthält, die subjektiv oder objektiv fehlerhaft sind (z.B. bei Verwechslungen). In diesem Fall kann der Patient seine Einwilligung

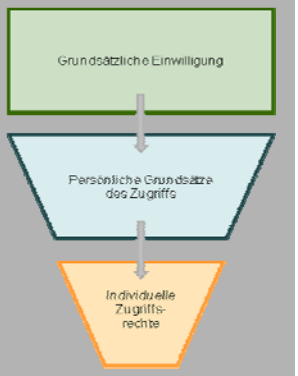
zur Teilnahme widerrufen oder die Dokumente der Vertraulichkeitsstufe "Geheim" zuordnen (siehe Empfehlung 4). In diesem Fall sind die Informationen nicht mehr abrufbar, gehen aber nicht verloren.

Empfehlung 3

Einwilligung und Zugriffsrechte

Der Patient, der dem Bereitstellen und Abrufen von Daten zustimmt, legt seinen Willen in Form von Einwilligungen fest. Jede Einwilligung bedingt eine Aufklärung des Patienten. Es werden drei Ebenen unterschieden :

- *Grundsätzliche Einwilligung:*
  Mit der grundsätzlichen Einwilligung zur Teilnahme im System «eHealth Schweiz» stimmt der Patient der Erstellung eines Patientendossiers mit dem zugehörigen Aufbau und der Ausgestaltung des Systems, den zugehörigen Grundlagen und Rahmenbedingungen sowie den allgemeinen Rechten und Pflichten der Teilnehmer zu.
  Mit der grundsätzlichen Einwilligung geht auch das Recht des Patienten einher, jederzeit auf seine Daten zugreifen zu können. Für die Regelung der Zugriffsrechte der übrigen Akteure werden die beiden folgenden Ebenen benötigt.



- *Persönliche Grundsätze unter Verwendung der Rollen:*
  Die Patienten können persönliche Grundsätze des Zugriffs festlegen. Dies kann über eine Kombination von Rollen und Vertraulichkeitsstufen erfolgen.

- *Individuelles Festlegen von Zugriffsrechten:*
  Der Patient kann die obigen Grundsätze durch spezielle Einzeleinstellungen übersteuern. Er kann
  - jedes Dokument individuell bezüglich Vertraulichkeit einstufen,
  - einzelne Behandelnde einer Rolle zuordnen und
  - einzelne Personen auf Ein- und Ausschlusslisten setzen.

Bei der Vertraulichkeit von Daten sind fünf Stufen vorgesehen (siehe Empfehlungen II „Standards und Architektur“ vom 21. Oktober 2010, Seite 24). Die Zuordnung eines Dokuments zur Vertraulichkeitsstufe wird nicht im Dokument, sondern als jederzeit änderbares Attribut (Metadaten) gespeichert.

Empfehlung 4

Definition der Vertraulichkeitsstufen

Daten, die den Patienten betreffen, sollen im Endausbau in die wie folgt definierten Vertraulichkeitsstufen unterteilt werden.

- *Administrative Daten:*
  Administrative Daten sind generell verfügbare Daten, welche nicht unter die folgenden vier Vertraulichkeitsstufen fallen, z.B. Name, Vorname, Geschlecht, Adresse, Geburtsdatum, Identifikatoren wie die eindeutige Kennzahl des Patienten und allenfalls weitere Kontaktdaten des Patienten,

- *Nützliche Daten:*
  Auf ausdrücklichen Wunsch des Patienten und im vom Patienten festgelegten Umfang: seine Verfügungen, Entscheidungen bezüg-

lich der Organspende, im Notfall zu benachrichtigende Personen sowie medizinische Daten, von denen im Gesundheitswesen anerkannt ist, dass alle Behandelnden einen direkten Zugriff haben sollten wie Allergien, spezifische Therapien (beispielsweise Gerinnungshemmer) oder besondere Erkrankungen wie Diabetes.

- *Medizinische Daten:*
  Dokumente und Daten, die den Patienten betreffen und für die künftige sichere Behandlung relevant sind, insbesondere Berichte und Befunde (z.B. Anamnese, Ergebnisse klinischer Untersuchungen, Analyseergebnisse, Situationsbeurteilungen, ‚vorgeschlagene und die tatsächlich durchgeführte Behandlungen).

- *Stigmatisierende Daten:*
  Medizinische Daten, deren Bekanntgabe gemäss eigener Einschätzung des Patienten (gegebenenfalls nach Beratung durch den Arzt des Vertrauens) seinem gesellschaftlichen oder privaten Leben schaden könnten.

- *Geheime Daten:*
  Der Patient kann veranlassen, dass Daten nur noch ihm zugänglich sind.

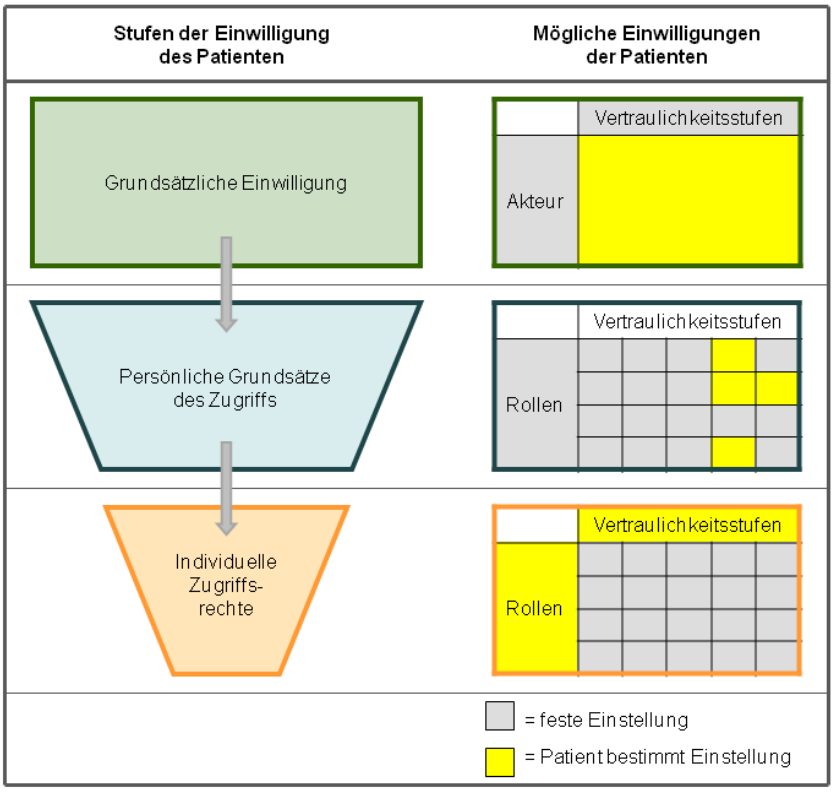


Abbildung 6: Stufen und mögliche Einwilligungen der Patienten

Zugang zu Dokumenten (Ableitung von Rechten aus der Matrix)

Beim Zugriff auf Daten werden die entsprechenden Zugriffsrechte immer an Personen im Kontext einer Rolle und nie an Institutionen vergeben. Ein Patient kann aber Zugriffsrechte an eine Gruppe aller Behandelnden eines Spitals verleihen. Auf die Vertraulichkeitsstufe "Geheim" gesetzte Daten sind nur noch für die betroffene Person auffindbar.

Das Rollenkonzept (siehe Empfehlungen II Teilprojekt Standards und Architektur, Kap. 3, S. 13ff.) ist Grundlage für das vorliegende Berechtigungskonzept. Auf der Basis des Rollenkonzepts können einer Person eine oder mehrere konkrete Rollen zugeordnet werden. Damit erhält die Person potentielle Rechte auf Zugriff. Alle zugelassenen Rollen werden in einem schweizweiten Verzeichnis mit einer eindeutigen Rollen-Identifikation geführt.

Bei der Publikation eines Dokumentes im elektronischen Patientendossier ist nicht im vornherein bekannt, wer zu welchem Zeitpunkt ein Dokument einsehen darf. Das System muss daher den Zugriff auf Dokumente in Abhängigkeit von der jeweiligen Behandlungssituation dynamisch ermitteln können. Die Rechte selbst werden in jeder Gemeinschaft in einem rollenbasierten Zugriffsberechtigungssystem verwaltet.

Der Patient als Besitzer der Dokumente hat immer Zugriff auf seine Dokumente, solange er die Vorbedingungen für eine Systemteilnahme erfüllt.

Personen als Träger von zugelassenen Rollen haben Zugriff gemäss Empfehlung 6.

Administrative Teilnehmer sind Mitarbeiter im Umfeld der Behandelnden (Administrativpersonal, Systembetreuer oder Helpdesk). Sie erhalten grundsätzlich nur Zugriff auf administrativen Daten.

Alle anderen Personen (Nicht-Teilnehmer) verfügen über keinen Zugriff auf das System.

Mit der Einwilligung zum Erstellen eines Patientendossiers und der Einwilligung zu den Zugriffsrechten gilt die folgende Grundeinstellung:

Empfehlung 5

Rechte bei der grundsätzlichen Einwilligung

Vertraulichkeitsstufe des Dokumentes Akteure	Administrative Daten	Nützliche Daten	Medizinische Daten	Stigmatisierende Daten	Geheime Daten
1. Patient	Ja	Ja	Ja	Ja	Ja
2. Behandelnde	Ja	Ja	siehe Empfehlung 6		
3. Administrativer Teilnehmer	Ja	Nein	Nein	Nein	Nein
4. Nicht-Teilnehmer	Nein	Nein	Nein	Nein	Nein

	Vertraulichkeitsstufen
Akteur	

Ja	Zugriff möglich
Nein	Zugriff nicht möglich

Tabelle 1: Berechtigungen der grundsätzlichen Einwilligung

Personalisierung der Matrix

Ergänzend zu den Voreinstellungen der grundsätzlichen Einwilligung kann der Patient die Berechtigungsregeln personalisieren. Auf der zweiten Ebene kann der Patient persönliche Grundsätze des Zugriffs festlegen und damit die für ihn spezifischen Zugriffsprinzipien definieren. Typischerweise legt er die Zugriffstiefe bezogen auf Vertraulichkeitsstufen für eine Rolle fest. Verschiedene vordefinierte Profile können ihm die Einstellung erleichtern.

Rollen in der Startphase

Die Akteure der Kategorie „Behandelnde“ (siehe Akteur 2 in Tabelle 1) können verschiedene Rollen wahrnehmen. Gemäss den Empfehlungen II ist dafür ein Verfahren zur Definition von Rollen vorzusehen. Diese verantwortlichen Stellen werden im Rahmen der Gesetzgebung des Bundes festgelegt. Für die Startphase werden in der Kategorie „Behandelnde“ die folgenden Rollen vorgeschlagen:

- *Mein Behandelnder:* Behandelnde mit direktem Bezug zur aktuellen Betreuung eines Patienten;
- *Behandelnder des Vertrauens:* Berater des Patienten im Zusammenhang mit den medizinischen Daten. Er erklärt dem Patienten die im Dossier enthaltenden Informationen und hilft ihm beim individuellen Festlegen der Zugriffsrechte;
- *Behandelnde allgemein:* Behandelnde ohne direkten Bezug zur aktuellen Betreuung eines Patienten;
- *Notfall-Behandelnder:* In Notfallsituationen können Behandelnde Daten ohne Einwilligung der Patienten abrufen. Die Patienten müssen nachträglich darüber informiert werden.

Empfehlung 6

Rechte unter Verwendung der Rollen

Vertraulichkeitsstufe des Dokumentes / Rollen	Administrative Daten	Nützliche Daten	Medizinische Daten	Stigmatisierende Daten	Geheime Daten
2.1 Mein Behandelnder	Ja	Ja	Ja	Option	Nein
2.2 Behandelnder des Vertrauens	Ja	Ja	Ja	Option	Option
2.3 Behandelnder allgemein	Ja	Ja	Nein	Nein	Nein
2.4 Notfall-Behandelnder	Ja	Ja	Ja	Option	Nein

Tabelle 2: Berechtigungen unter Verwendung der Rollen

Ja	Zugriff möglich
Nein	Zugriff nicht möglich
Option	Zugriff je nach individueller Einwilligung; Grundeinstellung: Nein

Empfehlung 7

Individuelle Festlegung der Zugriffsrechte

Auf der dritten Ebene werden alle Personen (inkl. und Gruppen von Personen) und nicht nur Behandelnde verwaltet. Hier stimmt der Patient durch individuelle Einwilligungen einer konkreten Datenspeicherung bzw. einem konkreten Datenzugriff zu. Er kann dabei namentlich einer Person eine bestimmte Rolle zuweisen oder entziehen und die Vertraulichkeit eines bestehenden Dokumentes ändern.

Die individuellen Festlegung der Zugriffsrechte ist jeweils definiert durch

a. die ausgewählten Behandelnden,
b. die zugewiesene (Behandelnden-) Rolle,
c. Anwendung von Ein- und Ausschlusslisten,
d. Dokumente, die über Metadaten gruppiert sind,
e. die Funktionen, die auf den Dokumenten möglich sind, wie z.B. Suchen, Lesen, etc.,
f. den Kontext, für den die Berechtigung gilt (z.B. Behandlungstyp Notfall), sowie
g. der Gültigkeitsdauer der Berechtigung.

Verwaltung der Einwilligungen

Zentrale Steuerung in dezentralen Gemeinschaften: Diese drei Berechtigungsebenen, besonders die individuelle Festlegung der Zugriffsrechte auf der dritten Ebene, verlangen, dass alle definierten individuellen Rechte eines Patienten an einem Ort verwaltet werden. Um dies in einer dezentralen Architektur möglich zu machen, müssen diese individuellen Rechte an einem Ort angesiedelt sein.

Alle Einwilligungen und Vergabe von Rechten eines Patienten werden in einer Gemeinschaft verwaltet. Diese Gemeinschaft wird als Stammgemeinschaft bezeichnet. Sie muss zwingend eine zertifizierte Gemeinschaft sein. Der Patient hat die freie Wahl, eine der zertifizierten Gemeinschaften als seine Stammgemeinschaft auszuwählen. Es gibt kein zentrales Register, in dem die Zugehörigkeit der Patienten zu ihrer Stammgemeinschaft geführt wird.	Empfehlung 8 Stammgemeinschaft
Eine Stammgemeinschaft kann auf Anfrage einer zertifizierten Gemeinschaft… ➢ … angeben, dass sie die Stammgemeinschaft zu einem bestimmten Patienten ist; ➢ … angeben, welche Einwilligungen und Zugriffsrechte (inklusive Black List) zu einem Patienten bestehen; ➢ … Einwilligungen und Zugriffsrechte zu verändern; ➢ … die Eigenschaft „Stammgemeinschaft“ einer Person an eine andere Gemeinschaft weitergeben (z.B. im Falle eines Umzugs).	Funktion einer Stammgemeinschaft
Der Stammgemeinschaft kommt eine Schlüsselfunktion zu. Aufgrund der Information aus der Stammgemeinschaft können Berechtigungen und Zugriffe durchgesetzt werden, denen ein Patient zugestimmt hat. Mit der Einwilligung zum Erstellen eines Patientendossiers wird die eröffnende Stelle automatisch zur Stammgemeinschaft. Wenn eine Gemeinschaft bei den anderen Gemeinschaften eine Abfrage macht, dürfen die verfügbaren Dokumente erst angezeigt werden, wenn aus der Stammgemeinschaft bekannt ist, welche Einwilligungen und Zugriffsrechte der Patient erteilt hat.	Aufgabe der Stammgemeinschaft
Alle Handlungen der Systemteilnehmer (inklusive Änderungen von Rollen / Berechtigungen) einer Gemeinschaft werden protokolliert. Jede Gemeinschaft führt ein eigenes Protokollierungssystem, das alle Handlungen aufzeichnet. Der Patient kann die Protokolleinträge (Zugriff auf Dokumente, Zugriff auf Metadaten) bezüglich Zugriff auf sein Patientendossier aus allen zertifizierten Gemeinschaften in einer verständlichen Form einsehen. Die Protokolleinträge dürfen nur Referenzen auf Personen und Dokumente enthalten und nicht Ausschnitte des Patientendossiers. Da die Protokolleinträge dennoch Rückschlüsse erlauben, müssen sie gleich behandelt werden wie die Daten und Dokumente des Patientendossiers selbst, d.h. die Zugriffe sind ebenso zu autorisieren.	Empfehlung 9 Nachverfolgbarkeit, Historisierung und Audit

4 Schlussbemerkungen

Nächste Schritte

In der folgenden Etappe werden die folgenden Themenbereiche, welche an die bisherigen Arbeiten anknüpfen, schwergewichtig bearbeitet:

- Schnittstelle administrative und medizinische Prozesse: Vertiefte Beschreibung zur Ausgestaltung der Schnittstelle zu administrativen Prozessen der Kostenträger, kommerzielle Gesundheitsakten, etc;
- Leitfaden für die Umsetzung der Empfehlungen I, II und III des Teilprojektes Standards und Architektur;
- Für jeden Service (z.B. Online-Abfragedienst Behandelnde, OID-Dienst, Verzeichnis der zertifizierten Gemeinschaften und Ermittlung der Stammgemeinschaft etc.) muss beschrieben werden, unter welchen Voraussetzungen er in Anspruch genommen werden kann (Zugangsvoraussetzungen, welche Daten werden unter welchen Voraussetzungen geliefert). Dies bedingt eine Entscheidung bezüglich des grundlegenden Architekturtypus und eine Festlegung der Zuständigkeiten und Verantwortlichkeiten;
- Weitere Empfehlungen für die Datensicherheit und den Datenschutz, z.B. Vertraulichkeit und Zugriff auf Protokolldaten oder das Thema von Administratorenrechten;
- Definition des Begriffs des Autors bzw. Publikationsverantwortlicher.

Einhaltung der Empfehlungen als Investitionsschutz

Der Steuerungsausschuss von „eHealth Suisse“ empfiehlt allen Akteuren im Sinne des Investitionsschutzes bei zukünftigen Neu- und Ersatzinvestitionen im IT-Bereich die Einhaltung der vom Teilprojekt "Standards und Architektur" empfohlenen technischen Lösungen und Ansätze im eigenen Verantwortungsbereich sicherzustellen.