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 V

Regeln für die Steuerung der Zugriffsrechte

Verabschiedet durch den Steuerungsausschuss

Bern, 28. August 2014

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

Impressum

Projektorganisation
Steuerungsausschuss: Alain Berset (Bundesrat, Vorsteher EDI); Pascal Strupler (Direktor BAG); Stefan Spycher (Vizedirektor BAG); Susanne Hochuli (Regierungsrätin, Vorsteherin GD AG, ab 01.07.2014); Carlo Conti (Regierungsrat, Vorsteher GD BS, bis 30.06.2014); Guido Graf (Regierungsrat, Vorsteher GD LU); Heidi Hanselmann (Regierungsrätin, Vorsteherin GD SG); Pierre-François Unger (Regierungsrat, Vorsteher GD GE, bis Ende 2013); Mauro Poggia (Regierungsrat, Vorsteher GD GE, ab Anfang 2014).
Projektleitungsgremium: Adrian Schmid („eHealth Suisse", Vorsitz); Christian Affolter (santésuisse bis Juli 2013); Lotte Arnold (SPO); Hansjörg Looser (GD SG); Daniel Notter (pharmaSuisse); Caroline Piana (H+); Georg Schielke (GDK); Adrian Jaggi (santésuisse ab Juli 2013); Walter Stüdeli (IG eHealth); Salome von Greyerz (BAG); Judith Wagner (FMH).

Geschäftsstelle „eHealth Suisse": Adrian Schmid (Leitung), Catherine Bugmann, Isabelle Hofmänner, Sang-Il Kim, Stefan Wyss, Corina von Känel

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

Das vorliegende Dokument enthält Vorschläge für die Steuerung der Zugriffsrechte auf das elektronische Patientendossier. Die Empfehlungen richten sich an Umsetzungsprojekte, welche die Zugriffsrechte der Patientinnen und Patienten strategiekonform ausgestalten wollen. Sie sind zudem ein möglicher Input für die Arbeiten des Bundes am Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier. Als Basis für die Empfehlungen diente eine Mandatsarbeit der „Arbeitsgemeinschaft Anwendungsfälle". Die Empfehlungsdokumente und die Vorbereitungsarbeiten sind zugänglich unter www.e-health-suisse.ch.

Veränderter rechtlicher Rahmen

Die bisherigen Empfehlungen von „eHealth Suisse" orientierten sich am geltenden Recht. Bei den vorliegenden Empfehlungen V wird darüber hinaus der rechtliche Rahmen berücksichtigt, den die aktuelle Version des Entwurfs zum „Bundesgesetz über das elektronische Patientendossier" (EPDG) nach dem Entscheid des Ständerats vom 12. Juni 2014 vorschlägt. Diese ist zugänglich unter http://www.parlament.ch/ab/frameset/d/s/4914/439277/d_s_4914_439277_439278.htm.

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

Fachliche Positionierung des Dokumentes

Das vorliegende Dokument beschreibt auf fachlicher Ebene, welche Regeln bei der Steuerung der Zugriffsrechte für das elektronische Patientendossier (EPD) gelten sollen. Voraussetzung für die 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.

Bisherige Empfehlungen als Basis

Grundlage sind die bisherigen Empfehlungen und Berichte von „eHealth Suisse“ - insbesondere die Empfehlungen I bis IV des Teilprojektes „Standards und Architektur“. Zum Thema „Zugriffssteuerung“ und „Zugriffsrechte“ sind dies insbesondere:

- *Architektur „eHealth Schweiz“:* In den Empfehlungen I (19. März 2009) wird die Basiskomponente „Zugriffssteuerung“ eingeführt, die mit einer rollenbasierten Umsetzung die Grundsätze des Datenschutzes sicherstellen soll;
- *Schweizweit koordinierte Komponente:* Die Empfehlungen II (21. Oktober 2010) positionieren die „Zugriffssteuerung“ als schweizweit zu koordinierende Basiskomponente. Gleichzeitig wird das Rollenkonzept eingeführt, das auf einer generischen Ebene festlegt, welche Informationen für welche Rolle zugänglich sind. Zusammen mit den fünf Vertraulichkeitsstufen von Dokumenten ist das Rollenkonzept ein wichtiges Instrument zur Verwaltung der Zugriffsrechte;
- *Einwilligung und Zugriffsrechte:* Die Empfehlungen III (27. Oktober 2011) unterscheiden drei Ebenen von Einwilligungen: „Grundsätzliche Einwilligung“, „Persönliche Grundsätze“ unter Verwendung der Rollen sowie „Individuelles Festlegen von Zugriffsrechten“. Die Rechtematrix kombiniert die möglichen Rollen für Behandelnde sowie die möglichen Vertraulichkeitsstufen für Dokumente. Auf dieser Basis kann festgelegt werden, welche Behandelnden auf Dokumente welcher Vertraulichkeitsstufen Zugriff haben;
- *Stammgemeinschaft verwaltet Zugriffsrechte:* Mit den Empfehlungen IV (17. Januar 2013) wird festgelegt, dass die Verwaltung der Zugriffsrechte dezentral in der jeweiligen Stammgemeinschaft des Patienten erfolgen soll. Das interne Zugangsportal der Stammgemeinschaft soll den Patienten die Verwaltung ihrer Zugriffsrechte ermöglichen.

Der Mensch steht im Zentrum und bestimmt selbst

Die „Strategie eHealth Schweiz" aus dem Jahr 2007 stellt den Menschen als Individuum und seine Bedürfnisse ins Zentrum. Zudem hat der Steuerungsausschuss von „eHealth Suisse" im Jahr 2009 die allgemeine Leitlinie verabschiedet, wonach „die Patientinnen und Patienten über den Umgang mit ihren Gesundheitsdaten entscheiden". Die „Expertengruppe eHealth" des EDI sowie der Entwurf zum Bundesgesetz über das elektronische Patientendossier (EPDG) bestätigten diese Linie. Bei der Definition der Zugriffsrechte ist somit darauf zu achten, dass der Patient stets die Kontrolle über den Zugriff auf seine Daten hat. Eine wichtige Grundlage für die Zugriffssteuerung ist die sogenannte „informierte Einwilligung" (vgl. Art. 3 Abs. 1 EPDG), die nach ausreichender Aufklärung über die Möglichkeiten, Rechte und Pflichten frei getroffene Einwilligung des Patienten. Diese Einwilligung steht immer am Anfang beim Eintritt eines Patienten ins EPD-System (siehe auch Kapitel 2.1 Grundprinzipien).

Varianten, bei denen die Gesundheitsfachpersonen (GFPs) ohne ausdrückliche Zustimmung der Patienten selber Zugriffsrechte erteilen oder ihre Zugriffsrechte weitergeben, erfüllen dieses Kriterium nicht. Transparenz und Vertrauen sind eine wichtige Voraussetzung für die Akzeptanz des elektronischen Patientendossiers (EPD). Zur Vereinfachung der Verwaltung der Zugriffsrechte kann den Patienten eine Auswahl von Voreinstellungen angeboten werden. Dadurch können Zugriffsrechte auf einfache Art verändert werden. Voraussetzung ist eine angemessene Information der Patienten.

1.2 Begriffe

Behandlungskontext

Im EPD-Kontext können medizinische Daten nur dann eingesehen werden, wenn der Behandlungskontext „explizit" durch den Patienten bestätigt wird. Also erst, wenn der Patient einer Gesundheitsfachperson das Zugriffsrecht erteilt hat.

Gesundheitsfachperson

Der Begriff Gesundheitsfachperson (GFP) ist in Artikel 2 Buchstabe b des EPDG wie folgt definiert: *„Gesundheitsfachperson: nach eidgenössischem oder kantonalem Recht anerkannte Fachperson, die im Gesundheitsbereich Behandlungen durchführt oder anordnet oder im Zusammenhang mit einer Behandlung Produkte abgibt,"*

Für den Zugriff auf das EPD-System muss eine Gesundheitsfachperson Mitglied einer zertifizierten Gemeinschaft sein. Das bedeutet:

- die Gesundheitsfachperson muss im nationalen Health Professional Index-Auskunftsdienst registriert sein,
- die Gesundheitsfachperson kann sich mit einer starken Authentisierung am EPD-System anmelden.

Im nachfolgenden Text wird der Begriff „Gesundheitsfachperson" für diejenigen Personen verwendet, die obige Bedingungen erfüllen und Mitglied einer zertifizierten Gemeinschaft sind.

Gruppe von Gesundheitsfachpersonen

Der Begriff „Gruppe von Gesundheitsfachpersonen“ umfasst alle in einer Gesundheitsorganisation und deren Unterorganisationen tätigen Gesundheitsfachpersonen, die Mitglied einer zertifizierten Gemeinschaft sind. Gesundheitsorganisationen können stationäre Einrichtungen wie akutsomatische oder Rehabilitations-Spitäler, Gruppen- oder Einzelpraxen, Apotheken oder Spitexorganisationen etc. sein. Darüber hinaus können sogenannte „virtuelle“ Gruppen von Gesundheitsfachpersonen von Bedeutung sein, zum Beispiel ein onkologisches Netzwerk aus Gesundheitsfachpersonen aus verschiedenen Organisationen (z.B. Tumorboard). Alle Gruppen müssen im Health Organisation Index (HOI) abgebildet werden.

Patientenadminstrator

Für die administrativen Prozesse rund um das EPD müssen die Patientenadministratoren einer Gemeinschaft Zugriff auf die demografischen Daten eines Patienten erhalten. Dies ist insbesondere für die richtige Identifikation des Patienten bei der Eröffnung des elektronischen Patientendossiers oder beim erstmaligen Kontakt des Patienten mit einer Gesundheitsorganisation von Bedeutung, um Patienten zu finden oder Verwechselungen zu vermeiden. Die Patientenadministratoren handeln im Sinne von „Hilfspersonen“ im Auftrag einer Gesundheitsfachperson.

Vertraulichkeitsstufen der EPD-Inhalte

In den Empfehlung III sind fünf Vertraulichkeitsstufen definiert worden (Empfehlung 4). Die Namensgebung wird angepasst, um Missverständnisse zu vermeiden:

- Demografische Daten (ehemals „administrative Daten“):

  Zum Beispiel Name, Vorname, Geschlecht, Adresse, Geburtsdatum, weitere Merkmale zur Identifikation wie zum Beispiel die Patientenidentifikationsnummer nach EPDG und allenfalls weitere Kontaktdaten des Patienten;

- Nützliche Daten:

  Zum Beispiel Informationen über Allergien und Unverträglichkeiten, spezifische Therapien (beispielswiese Gerinnungshemmer), besondere Erkrankungen (z.B. Diabetes), aber auch Patientenverfügung, Organspendeausweis, im Notfall zu benachrichtigende Personen;

- Medizinische Daten:

  Dokumente und Daten, die den Patienten betreffen und für eine sichere Behandlung relevant sind, insbesondere Berichte und Befunde (zum Beispiel Anamnese, Ergebnisse klinischer Untersuchungen, Analyseergebnisse, Situationsbeurteilungen, vorgeschlagene und die tatsächlich durchgeführte Behandlungen);

- Sensible Daten (ehemals „stigmatisierende Daten“):

  Medizinische Daten, deren zu breite Bekanntgabe gemäss eigener Einschätzung des Patienten seinem gesellschaftlichen oder privaten Leben schaden könnten;

- Geheime Daten:

  Medizinische Daten, die nur der Patient selbst einsehen kann.

Abbildung 1 zeigt, dass verschiedene EPD-Inhalte jederzeit durch den Patienten in andere Vertraulichkeitsstufen verschoben werden können.

Alle Inhalte des EPD müssen in eine der fünf Vertraulichkeitsstufen eingeteilt werden. Jeder neue EPD-Inhalt erhält eine Vertraulichkeitsstufe, die in der Grundeinstellung festgelegt ist, die im Ausführungsrecht zum EPDG definiert wird. Diese Einstellung kann vom Patienten angepasst werden.

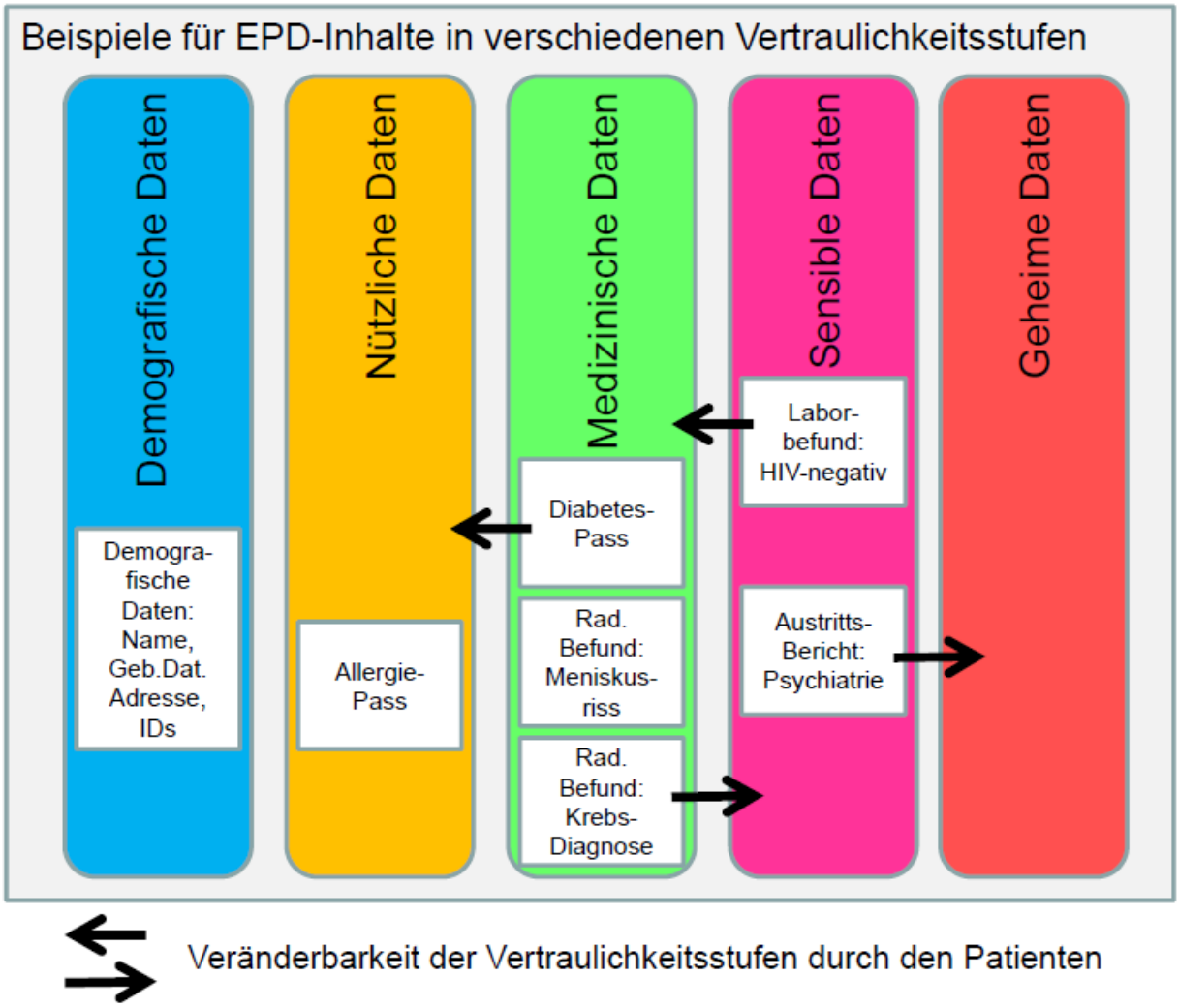

Abbildung 1: Vertraulichkeitsstufen und ihre Veränderbarkeit (fiktives Beispiel)

Rechtematrix

Die vom Patienten gewählten Zugriffsregeln werden in Form einer Rechtematrix aus der Kombination von berechtigter Person mit zugeteilter Zugriffsstufe und Vertraulichkeitsstufen der EPD-Inhalte festgehalten. Für die Entscheidung, ob ein Zugriff auf ein Dokument erteilt oder verweigert wird, müssen diese Regeln ausgewertet werden. Die berechtigten Personen (Gesundheitsfachpersonen und Patienten) haben Zugriff aufs EPD, wenn die erforderlichen Bedingungen erfüllt sind. Die Rechtematrix kann jederzeit vom Patienten angepasst werden.

Grundeinstellung

Die Grundeinstellung der Zugriffsrechte gilt für alle neu eröffneten EPDs. In der Grundeinstellung werden eine Rechtematrix und weitere Regeln, zum Beispiel zeitliche Befristung der Zugriffsrechte oder Regeln für das Setzen der Vertraulichkeitsstufen, festgelegt. Alle Einstellungen der Grundeinstellung können durch den Patienten jederzeit verändert werden.

Voreinstellungen

Voreinstellungen der Zugriffssteuerung entsprechen Zusammenfassungen von einzelnen Einstellungen. Diese Voreinstellungen sollen den Patienten die Verwaltung der Zugriffsrechte auf sein EPD erleichtern, damit er nicht jede einzelne Einstellung manuell anpassen muss. Die Grundeinstellung kann als besondere Voreinstellung angesehen werden. Auch Voreinstellungen können durch den Patienten jederzeit verändert werden.

Zentrale Abfragedienste

Damit die elektronische Kommunikation zwischen den Gemeinschaften funktionieren kann, müssen die nachfolgend aufgeführten zentralen Abfragedienste in schweizweit koordinierter Form betrieben und deren Daten in verlässlicher und zeitnaher Qualität bereitgestellt werden. Dazu gehören insbesondere:

- Verzeichnis der Gesundheitsfachpersonen (HPI-Dienst);
- Verzeichnis der Gesundheitsorganisationen und Gruppen von Gesundheitsfachpersonen (HOI-Dienst).

Patienten Zugangsportal

Gemäss den „Standards und Architektur Empfehlungen IV“ vom 17. Januar 2013 kann die Verwaltung der individuellen Zugriffsrechte durch den Patienten nur über das interne Zugangsportal seiner Stammgemeinschaft erfolgen.

Zugriffsstufen anstatt Rollen

Die ehemaligen Rollenbezeichnungen aus „Standards und Architektur Empfehlungen III“ werden für ein besseres Verständnis umbenannt in unterschiedliche Zugriffsstufen (Access-Levels). Der Patient muss den Gesundheitsfachpersonen explizit eine Zugriffsstufe zuordnen, bevor diese die EPD-Inhalte einsehen können. Der Patient kann die Zugriffsstufe jederzeit ändern oder entziehen:

- Zugriffsstufe „administrativ“, ehemals Rolle „Administrative Teilnehmer“:
  Ermöglicht ausschliesslich den Zugriff auf die Daten der Vertraulichkeitsstufe „Demografische Daten“;
- Zugriffsstufe „eingeschränkt“(ehemals Rolle „Behandelnde allgemein“):
  Ermöglicht den Zugriff auf die Vertraulichkeitsstufen „Demografische Daten“ und „Nützliche Daten“;
- Zugriffsstufe „normal“ (ehemals Rolle „Mein Behandelnder“):
  Ermöglicht den Zugriff auf die Vertraulichkeitsstufen „Demografische Daten“, „Nützliche Daten“ sowie „Medizinische Daten“;
- Zugriffsstufe „erweitert“ (ehemals Rolle „Mein Behandelnder des Vertrauens“):
  Ermöglicht den Zugriff auf die Vertraulichkeitsstufen „Demografische Daten“, „Nützliche Daten“, „Medizinische Daten“ sowie „Sensible Daten“;

- Zugriffsstufe „Notfall“ (ehemals Rolle „Notfall-Behandelnder“): Ermöglicht im Falle eines medizinischen Notfalls auch ohne vorgängig erteiltes Zugriffsrecht durch den Patienten den Zugriff auf die Vertraulichkeitsstufen „Demografische Daten“, „Nützliche Daten“ sowie „Medizinische Daten“. Der Patient ist über die erfolgten Zugriffe nachträglich zu informieren. Der Patient kann den Zugriff in medizinischen Notfallsituationen jederzeit untersagen oder auf die Vertraulichkeitsstufen „Demografische Daten“ und „Nützliche Daten“ einschränken;
- Zugriffsstufe „gesamt“:

  Diese Zugriffsstufe ist dem Patienten vorbehalten. Somit kann der Patient alle Daten aller Vertraulichkeitsstufen, insbesondere auch die Vertraulichkeitsstufe „Geheim Daten“, einsehen. Es ist nicht vorgesehen, dass diese Zugriffsstufe über die Rechtematrix verändert werden kann.

2 Grundprinzipien und Regelwerk

2.1 Grundprinzipien

EPD ist Sekundärsystem

Das EPD-System dient einerseits dem Patienten als Sammlung seiner wichtigsten medizinischen Daten, auf die er jederzeit Zugriff hat. Andererseits verbessert das EPD den Informationsaustausch zwischen den Gesundheitsfachpersonen. Das EPD ist somit kein Primärsystem des Behandelnden (zum Beispiel Klinik-Informationssystem oder Arztpraxis-Informationssystem), in dem das interne medizinisches Handeln dokumentiert wird. Das EPD ist ein Sekundärsystem, in dem jene Informationen abgelegt sind, die für die Weiterbehandlung bei anderen Gesundheitsfachpersonen relevant sind. Die EPD-Zugriffssteuerung sagt nichts darüber aus, wie der Zugriff auf die Patientendaten in den Primärsystemen geregelt ist. Bei Primärsystemen werden die Zugriffsregeln innerhalb der Organisationen festgelegt. Die nachfolgenden Überlegungen betreffen somit nur das EPD als Sekundärsystem, das potentiell von mehr Personen eingesehen werden kann und den Zugang gibt zu teilweise langjährigen Informationen aus allen medizinischen Fachbereichen.

Grundprinzipien Zugriff

Mit der Einwilligung zur Eröffnung eines EPD nach angemessener Information und Aufklärung („Informed Consent“) akzeptiert der Patient die Grundprinzipien zur Steuerung der Zugriffsrechte. Er ist sich insbesondere über die Möglichkeiten, Rechte und Pflichten aller EPD-Akteure bewusst. Zu den Grundprinzipien gehören:

- Explizite Einwilligung, ein EPD zu führen (opt-in Modell) mit jederzeitigem Recht auf Widerruf;
- Eine definierte Zugriffsstufe kann nur Gesundheitsfachpersonen (inklusive deren Hilfspersonen), die im nationalen "Health Professional Index" (HPI) geführt werden und somit Mitglied einer zertifizierten Gemeinschaft sind und eine elektronische Identität besitzen, zugewiesen werden;
- Explizite Zuweisung einer Zugriffsstufe an Gesundheitsfachpersonen. Welche Vertraulichkeitsstufen für welche Zugriffsstufen sichtbar sind, bestimmt der Patient (über die Rechtematrix);
- Möglichkeit des individuellen Ausschlusses von Gesundheitsfachpersonen (Ausschlussliste);
- Der Zugriff auf ein Dokument im EPD wird zum Zeitpunkt der Anfrage durch Auswertung der Rechtematrix geprüft;
- Möglichkeit zum Notfallzugriff für Gesundheitsfachpersonen, die im HPI geführt werden, ohne vorgängige explizite Zuweisung von Zugriffsrechten durch den Patienten. Ob ein Notfallzugriff möglich ist und welche Vertraulichkeitsstufen sichtbar sind, bestimmt der Patient.

Die genannten Grundprinzipien der Zugriffssteuerung gelten für den Datenzugriff nach Eröffnung eines EPD. Die Anwendungsfälle „Eröffnung eines EPD“ und „Verändern der administrativen Daten im EPD“ und die sich daraus ergebenden Anforderungen werden hier nicht behandelt.

Aufbau der Zugriffssteuerung

Gemäss den Empfehlungen III basiert die EPD-Zugriffssteuerung auf drei Elementen (siehe Abbildung 4):

- Schriftliche Einwilligung in die Eröffnung eines elektronischen Patientendossiers nach erfolgter Aufklärung (Informed Consent);
- Festlegen der persönlichen Grundeinstellung der Rechtematrix und der Grundeinstellung der Vertraulichkeitsstufe für neu erfasste Dokumente (persönliche Grundsätze);
- Explizite Zuweisung der Zugriffsstufen an Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen sowie Änderung der Vertraulichkeitsstufen einzelner Dokumente (individuelle Einstellungen).

Abbildung 2: Aufbau der Zugriffssteuerung

2.2 Regelwerk

Regelwerk

Die Grundprinzipien können in einem Regelwerk abgebildet werden. Die folgende Beschreibung ist eine fachliche Definition auf abstrakter Ebene und keine Vorgabe für die technische Implementierung. Die Gemeinschaften bleiben in der internen Ausgestaltung der Umsetzung frei, solange die Logik des beschriebenen Regelwerks korrekt erfüllt wird.

Die Grundidee des Regelwerks besteht in einem dreistufigen Verfahren mit

- Prüfung von Ausschlusskriterien,
- Einschlusskriterien und der
- Rechtematrix.

In einer ersten Stufe werden sogenannte Ausschlusskriterien überprüft. Trifft eines der Kriterien zu (ist zum Beispiel die anfragende Gesundheitsfachperson auf der Ausschlussliste des Patienten), wird der Zugriff ohne weitere Prüfungen verweigert.

Wenn keines der Ausschlusskriterien den Zugriff verweigert, werden in einer zweiten Stufe sogenannte Einschlusskriterien überprüft. Trifft mindestens eines der Einschlusskriterien zu (zum Beispiel hat die anfragende Gesundheitsfachperson vom Patienten eine entsprechende Zugriffsstufe zugewiesen bekommen), dann erfolgt die Prüfung auf Stufe drei. Trifft kein Einschlusskriterium zu, wird der Zugriff ebenfalls verweigert.

In der dritten Stufe muss die persönliche Rechtematrix ausgewertet werden, also die Kombination von Zugriffsstufe der anfragenden Gesundheitsfachperson und der Vertraulichkeitsstufe der im EPD erfassten Dokumente.

In Abbildung 3 ist das dreistufige Regelwerk schematisch dargestellt:

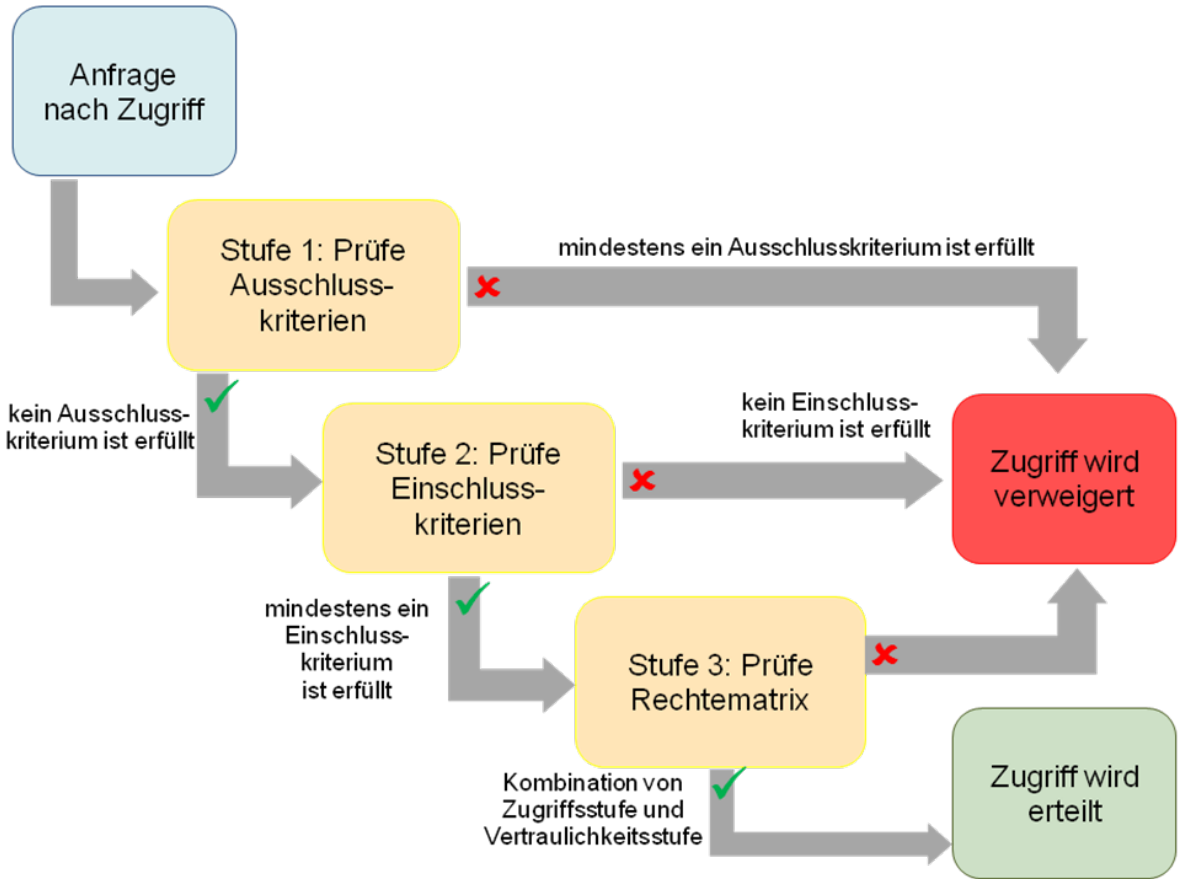

Abbildung 3: Dreistufiges Regelwerk

Vor dem Zugriff auf das EPD werden Ausschlusskriterien, Einschlusskriterien und die Rechtematrix geprüft. Damit ein Zugriff erteilt wird, darf kein Ausschlusskriterium zutreffen UND es muss mindestens ein Einschlusskriterium erfüllt sein UND es muss der Zugriff gemäss Rechtematrix erlaubt sein.	Empfehlung 1 Dreistufiges Regelwerk
Aus den anfangs genannten Grundprinzipien lassen sich zwei Ausschlusskriterien ableiten:	Prüfung Ausschlusskriterien

1. Die Einwilligung des Patienten ist Voraussetzung für das Erstellen und Führen eines EPD (opt-in Modell). Diese Einwilligung kann der Patient jederzeit widerrufen und damit sämtliche Zugriffsmöglichkeiten sperren.

2. Der Patient kann jederzeit einzelne Gesundheitsfachpersonen vom Zugriff auf sein EPD ausschliessen. Dafür wird eine Ausschlussliste erstellt. Diese Ausschlussliste übersteuert alle anderen Regeln.

Abbildung 4 zeigt schematisch die einzelnen Prüfschritte:

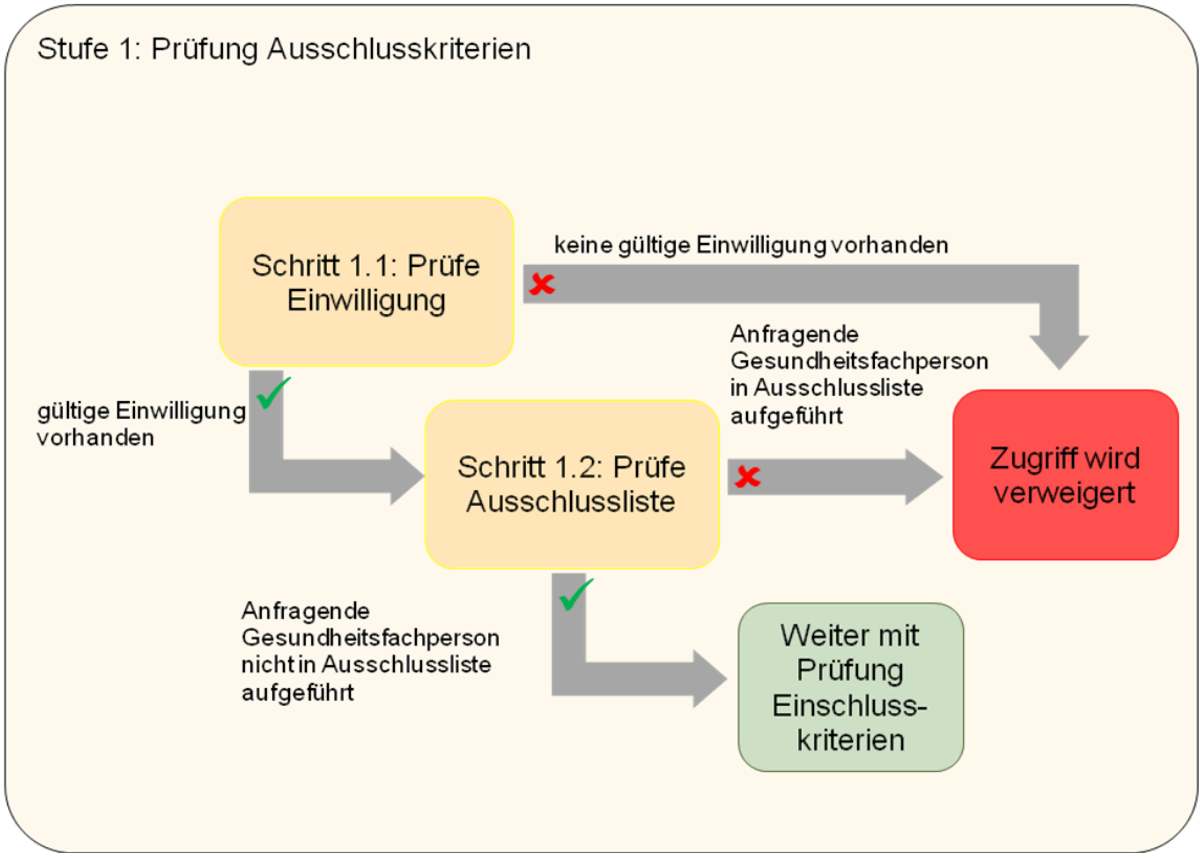

Abbildung 4: Regelwerk - Ausschlusskriterien (Zoom in „Stufe 1“ aus Abbildung 3)

Folgende Ausschlusskriterien werden geprüft und verhindern den Zugriff: ➢ Eine Einwilligung zum Führen eines EPD ist nicht vorhanden, da der Patient seine Einwilligung widerrufen hat; ➢ Die anfragende Gesundheitsfachperson ist in der Ausschlussliste des Patienten aufgeführt.	Empfehlung 2 Ausschlusskriterien
Bei der Prüfung der Einschlusskriterien ist die Beziehung zum Patienten relevant, in der sich die anfragende Gesundheitsfachperson zum Zeitpunkt der Anfrage befindet. Es können zwei verschiedene Fälle unterschieden werden, die als Einschlusskriterium überprüft werden. Trifft einer zu, wird in der dritten Stufe die Rechtematrix ausgewertet. Folgende zwei Fälle müssen gemäss der unten stehenden Abbildung 5 überprüft werden:	Prüfung Einschlusskriterien

Zwei Fälle bei Einschlusskriterien

Fall 1:

Ist die anfragende Gesundheitsfachperson namentlich durch Zuweisung einer Zugriffsstufe berechtigt worden? Falls dieses Kriterium zutrifft, darf die anfragende Gesundheitsfachperson, passend zu ihrer Zugriffsstufe, die entsprechenden Vertraulichkeitsstufen gemäss der Rechtematrix des Patienten einsehen.

Fall 2:

Handelt es sich bei der Anfrage um einen Notfallzugriff? In diesem Fall wird der anfragenden Gesundheitsfachperson die Zugriffsstufe „Notfall“ zugewiesen, sobald sie den Notfallzugriff bestätigt. Danach darf sie die freigegebenen Vertraulichkeitsstufen einsehen, sofern der Patient den Notfallzugriff nicht ausdrücklich ausgeschlossen hat. Hier besteht ein besonderer Behandlungskontext, da die Gesundheitsfachperson den Notfallzugriff in Anspruch nimmt und sich die Zugriffsstufe „Notfall“ selbst zuweist.

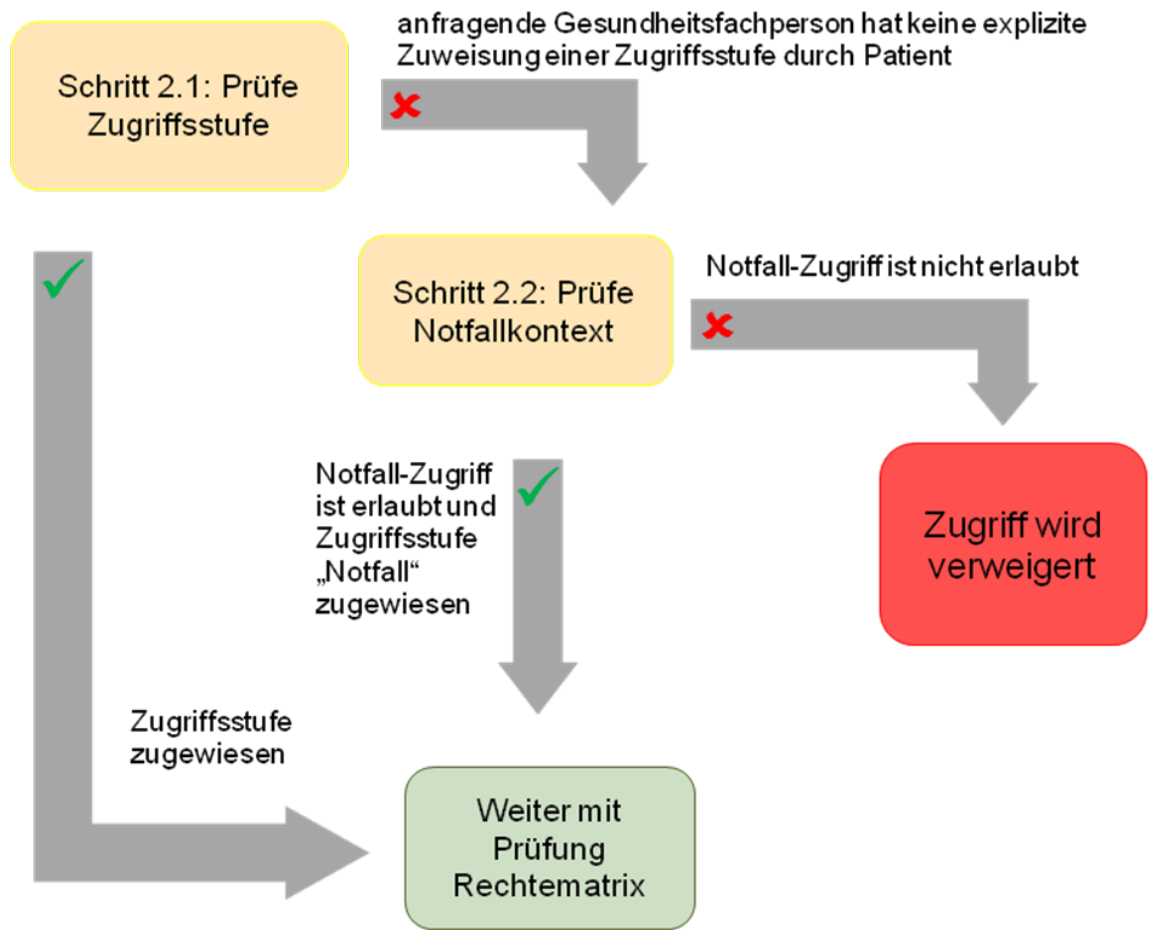

Abbildung 5: Regelwerk - Einschlusskriterien (Zoom in „Stufe 2“ aus Abbildung 3)

Folgende Einschlusskriterien werden geprüft: ➢ Behandlungskontext: Der Patient legt fest, wer zum Kreis seiner Behandelnden gehört. Er weist passende Zugriffsstufen explizit den gewünschten Gesundheitsfachpersonen zu. ➢ Notfallkontext: In medizinischen Notfallsituationen können Gesundheitsfachpersonen auch ohne vorgängig vergebene Zugriffsrechte auf Daten aus dem EPD zugreifen. Der anfragenden Gesundheitsfachperson wird die Zugriffsstufe „Notfall“ zugewiesen. Der Patient kann die sichtbaren Vertraulichkeitsstufen für den Notfallzugriff festlegen. Eine Gesundheitsfachperson kann den Notfallzugriff beanspruchen. Dieser Zugriff betrifft nur das Dossier des ausgewählten Patienten. Der Patient wird über den Zugriff aktiv informiert.	Empfehlung 3 Einschlusskriterien
In der dritten und letzten Stufe wird die persönliche Rechtematrix des Patienten ausgewertet. Welche Daten und Dokumente tatsächlich zugänglich sind, hängt von der Zugriffsstufe der anfragenden Gesundheitsfachperson, den Vertraulichkeitsstufen der im EPD erfassten Dokumente und von den Regeln ab, die der Patient in seiner Rechtematrix eingestellt hat.	Auswertung Rechtematrix

2.3 Grundeinstellung und Voreinstellungen

Das Grundprinzip der Zugriffssteuerung wurde in den vorhergehenden Empfehlungen definiert und gilt für alle Anwendungsfälle. Mit der Eröffnung eines EPD gilt eine rechtlich festgelegte Grundeinstellung für die Steuerung von Zugriffsrechten. Diese Grundeinstellung soll eine ausgewogene Balance sein zwischen datenschutzrechtlichen Vorgaben, dem Sicherheitsempfinden von weiten Kreisen der Bevölkerung sowie dem sinnvollen Einsatz und Nutzen der EPD-Daten für eine bessere und sichere Behandlung der Patienten. Der Patient kann diese Einstellung jederzeit seinen individuellen Bedürfnissen anpassen, insbesondere unmittelbar nach Eröffnung seines EPDs. Damit nicht jede Einstellung der Zugriffssteuerung einzeln angepasst werden muss, können dem Patienten Voreinstellungen der Zugriffssteuerung angeboten werden, die von der Grundeinstellung abweichen. Damit können jene Patienten unterstützt werden, die auf einfache Weise eine offenere oder restriktivere Einstellung ihrer Zugriffsrechte festlegen wollen. Der Entscheid für ein Modell, das von der Grundeinstellung abweicht, schliesst spätere individuelle Anpassungen durch den Patienten nicht aus.	Grundsatz
Nach der grundsätzlichen Einwilligung und Eröffnung eines EPD gilt die rechtlich festgelegte Grundeinstellung der Zugriffsrechte. Der Patient kann aus weiteren Voreinstellungen auswählen. Alle Einstellungen können vom Patienten jederzeit individuell angepasst werden.	Empfehlung 4 Definierte Grundeinstellung, Auswahl Voreinstellungen
Die Vergabe von Zugriffsrechten ist immer zeitlich limitiert und richtet sich nach dem Behandlungskontext. Die zugreifenden Gesundheitsfachpersonen sollen solange über das Zugriffsrecht verfügen, wie es für eine optimale Behandlung sinnvoll und verhältnismässig ist. Im Grundsatz bestimmt der Patient die Dauer der vergebenen Zugriffsrechte.	

In der Grundeinstellung sind die Zugriffsrechte zeitlich befristet. Der Patient kann diese Fristen jederzeit verändern oder aufheben.	Empfehlung 5 Zeitliche Begrenzung von Zugriffsrechten
Im Prozess der Steuerung der Zugriffsrechte spielt die Vergabe der Vertraulichkeitsstufe eines Dokumentes und die Auswertung dieses Attributes eine zentrale Rolle. Die Regeln für die Vergabe der initialen Vertraulichkeitsstufen bei der Veröffentlichung der Dokumente im EPD sind Teil der Grundeinstellung. Gemäss den Grundprinzipien kann der Patient jederzeit die Vertraulichkeitsstufe jedes einzelnen Dokuments verändern. Für eine höhere Praktikabilität der Verwaltung der Vertraulichkeitsstufen können die Patienten auf Basis von Dokumenten-Metadaten summarisch einfache und verständliche Regeln aufstellen.	Setzen von Vertraulichkeitsstufen
Der Patient kann jederzeit Regeln für das summarische Setzen der Vertraulichkeitsstufe von Dokumenten definieren. Das Zugangsportal seiner Stammgemeinschaft bietet diese Funktion an.	Empfehlung 6 Regeln für Setzen von Vertraulichkeitsstufen
Um die Kontrolle des Patienten über seine EPD-Inhalte sicherzustellen, werden die Empfehlungen 5+6 aus den „Empfehlungen III“ des Teilprojektes Standards und Architektur vom 27. Oktober 2011 angepasst. Durch die Zugriffsmöglichkeit auf die demografischen Daten des Patienten wird gewährleistet, dass Patientenadministratoren (Hilfspersonen) und Gesundheitsfachpersonen die entsprechenden Patienten im EPD-System finden und eindeutig identifizieren können. Zudem soll nur der Patient selbst Dokumente der Vertraulichkeitsstufe „Geheime Daten“ einsehen können. Falls Dokumente mit der Vertraulichkeitsstufe „Geheime Daten“ zugänglich gemacht werden sollen, muss der Patient entsprechend die Vertraulichkeitsstufe des Dokumentes auf „Sensible Daten“ oder „Medizinische Daten“ ändern.	Anpassungen Empfehlung 5 und 6 aus „Empfehlungen III“
Die Rechtematrix und die dargestellte Grundeinstellung ist bei Eröffnung eines EPD anzuwenden. Der Patient kann die veränderbaren Felder der Matrix jederzeit ändern. Es gilt die Regel, dass weniger restriktive Einstellungen der Vertraulichkeitsstufe immer mit eingeschlossen sind.	Empfehlung 7 Anwendung der Rechtematrix

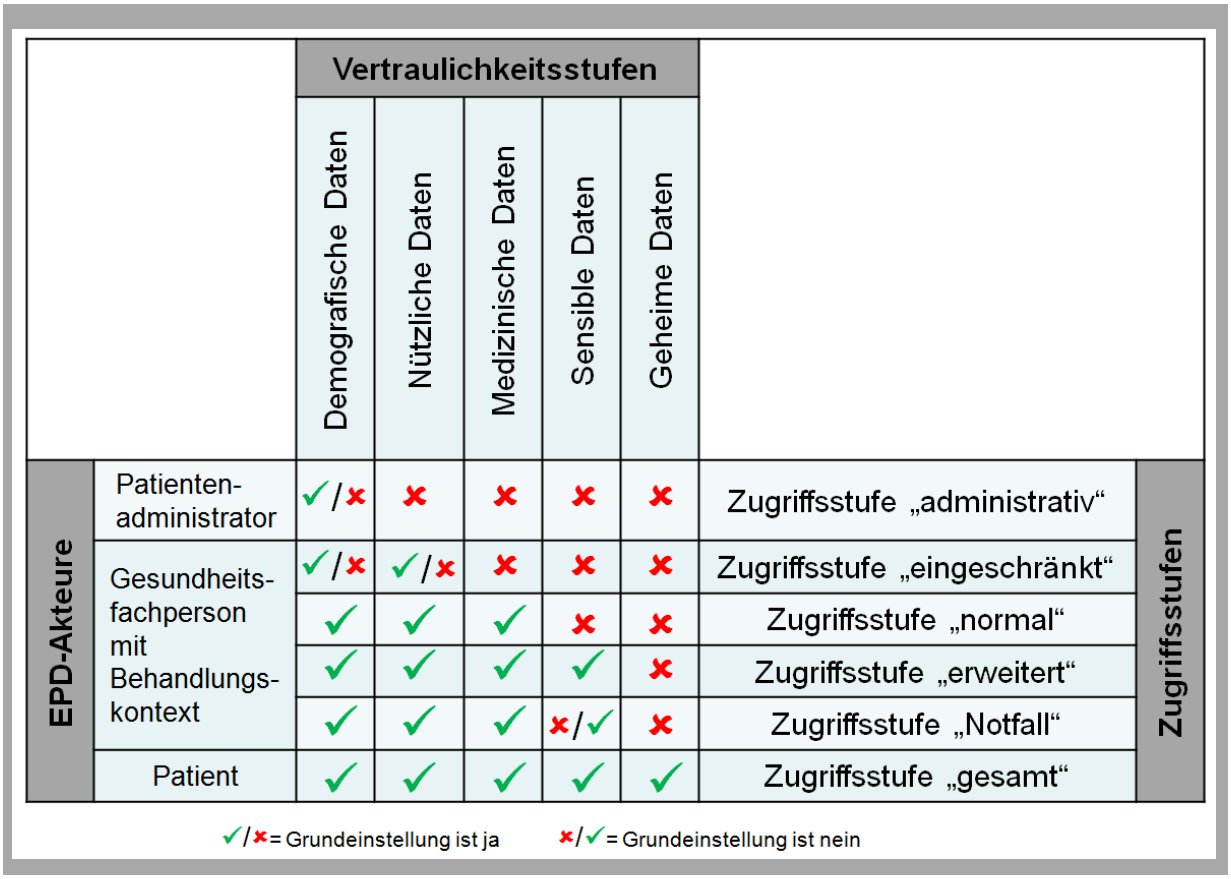

Abbildung 6: Grundeinstellung

Hinweis: Bei jeder Grundeinstellung oder Voreinstellung gilt immer der Grundsatz „Explizite Zuweisung einer Zugriffsstufe an eine Gesundheitsfachperson für den Zugriff auf EPD-Inhalte“ (siehe auch Empfehlung 3). „Automatische Zugriffsrechte“ sind nicht möglich.

2.4 Ermächtigung und Stellvertretung

Nutzen der Ermächtigung

In gewissen Situationen kann es für den Patienten sinnvoll sein, das Recht auf Zuweisung einer Zugriffsstufe an eine Gesundheitsfachperson stellvertretend auch seinen Behandelnden zu erteilen. Der Ermächtigungsprozess muss elektronisch erfolgen. Das bedeutet, dass der Ermächtigungsprozess elektronisch verifiziert, dokumentiert und protokolliert werden muss.

Weil die Rechtematrix nur innerhalb einer Stammgemeinschaft verändert werden kann, können vom Patienten nur Gesundheitsfachpersonen seiner Stammgemeinschaft ermächtigt werden, stellvertretend anderen Gesundheitsfachpersonen eine Zugriffsstufe zuzuweisen. Die neu zugriffsberechtigten Gesundheitsfachpersonen können sowohl in der eigenen Stammgemeinschaft oder in einer anderen Gemeinschaft sein.

Der Patient kann Gesundheitsfachpersonen seiner Stammgemeinschaft ermächtigen, an seiner Stelle einer anderen Gesundheitsfachperson eine Zugriffsstufe zuzuweisen. Die ermächtigten Gesundheitsfachpersonen können maximal nur die Zugriffsstufe zuweisen, welche sie zu diesem Zeitpunkt selber besitzen. Der Ermächtigungsprozess muss elektronisch erfolgen und entsprechend protokolliert werden. Eine Ermächtigung ist zeitlich beschränkt und kann jederzeit durch den Patienten widerrufen werden. Die Ermächtigung, in Vertretung des Patienten Zugriffsstufen zuzuweisen, kann von den Gesundheitsfachpersonen nicht weitergegeben werden. Der Patient wird über alle Anfragen und Vergaben von Zugriffsrechten informiert.	Empfehlung 8 Ermächtigung zur Zuweisung von Zugriffsstufen
Besucht ein Patient eine Gesundheitsfachperson, die stellvertretend tätig ist (zum Beispiel wegen Abwesenheit oder Urlaub), sieht die Zugriffssteuerung keinen speziellen Mechanismus vor. In diesem Fall muss der Patient der Stellvertretung seines Behandelnden explizit die Zugriffsrechte erteilen.	Stellvertretung des Behandelnden
Bei der Stellvertretung eines Patienten wegen Urteilsunfähigkeit oder Unmündigkeit gelten die üblichen zivilrechtlichen Regeln.	Stellvertretung des Patienten

2.5 Zugriffsrechte für Gruppen von Gesundheitsfachpersonen

Im Behandlungsprozess sind häufig Institutionen und Organisationen oder virtuelle Gruppen involviert, zum Beispiel eine Gemeinschaftspraxis, Stationen im Spital, Spitex-Dienste oder ein fachliche Expertengruppen (zum Beispiel ein „Tumorboard“). Solchen Organisationen oder Gruppen von Gesundheitsfachpersonen soll das Zugriffsrecht auf das EPD eines Patienten gewährt werden können.	Gruppenaspekt
Dazu soll dem Patienten die Möglichkeit gegeben werden, Gruppen von Gesundheitsfachpersonen in einem Abfragedienst zu finden und summarisch allen Mitgliedern dieser Gruppe die Zugriffsrechte zu erteilen. Der Patient kann dabei einzelne Gesundheitsfachpersonen aus einer Gruppe vom Zugriff ausschliessen. Es dürfen bei Gruppenberechtigungsvergaben innerhalb der jeweiligen Gruppe nur jene Personen auf das EPD eines Patienten zugreifen, welche die darin enthaltenen Daten für ihre Arbeit benötigen, gemäss dem Grundsatz „Zugang ist zulässig, sofern zur Aufgabenerfüllung notwendig“.	Benutzbarkeit für den Patienten
In einem Abfragedienst muss ersichtlich sein, aus welchen Gesundheitsfachpersonen sich eine Gruppe zusammensetzt. Dieser Abfragedienst heisst „Health Organisation Index“-Dienst (HOI-Dienst). Ein Tumorboard zum Beispiel kann als eine „virtuelle Gruppe“ im HOI aufgeführt sein. Eine Gesundheitsfachperson kann mehr als einer Gruppe angehören.	Gruppen und HOI-Abfragedienst
Um das Management der Zugriffsrechte zu vereinfachen, können Gruppen von Gesundheitsfachpersonen gebildet werden. Die Mitglieder einer Gruppe müssen im HOI abgebildet sein. Verantwortlich für die Pflege einer Gruppe ist die anmeldende Stelle in der zertifizierten Gemeinschaft.	Empfehlung 9 Abbildung einer Gruppe im HOI-Abfragedienst

Alle im HPI registrierten Gesundheitsfachpersonen müssen von ihren Organisationen darüber informiert werden, wenn sie namentlich als Mitglieder einer Gruppe im HOI aufgeführt werden sollen. Aus Datenschutzgründen können die Gesundheitsfachpersonen darauf verzichten.

Informationspflichten der Organisationen

2.6 Bereitstellung von Dokumenten im ePatientendossier

Wenn eine Person in die Eröffnung eines EPD einwilligt, so wird gemäss EPDG im Behandlungsfall vermutet, dass diese Person der Erfassung der behandlungsrelevanten Daten im EPD zustimmt. Die Gemeinschaften müssen sicherstellen, dass diese Daten für Gesundheitsfachpersonen mit den entsprechenden Zugriffsrechten über das EPD zugänglich sind. Es besteht somit keine zwingende Verknüpfung zwischen Lese- und Schreibrechten.

Im Behandlungsfall wird vermutet, dass der Patient der Bereitstellung der behandlungsrelevanten Daten im EPD zustimmt. Das Einholen einer expliziten Einwilligung ist nicht notwendig.	Empfehlung 10
Der Patient kann sich jedoch jederzeit gegen die Bereitstellung gewisser Dokumente aussprechen. Er muss die entsprechenden Gesundheitsfachpersonen über seinen Entscheid informieren.	Bereitstellung von Dokumenten

3 Schlussbemerkungen und offene Fragen

Fazit

Die Empfehlungen V konkretisieren die Regeln für die Steuerung der Zugriffsrechte im EPD. Dabei ist es das übergeordnete Ziel, dass der Patient die Kontrolle über seine Daten besitzt und bestimmt, wer mit diesen arbeiten darf. Gleichzeitig sollte eine sinnvolle Balance zwischen den datenschutzrechtlichen Anforderungen, Benutzbarkeit und Behandlungssicherheit gefunden werden. Die Zugriffssteuerung soll für den Patienten leicht benutzbar sein und im Interesse der Patientensicherheit Instrumente vorsehen, die den Datenzugang für involvierte Behandelnde im medizinischen Bedarfsfall auf eine praktikable Weise möglich machen.

Nächste Schritte

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

- Definition des Rechteattribute-Sets mit Konkretisierung der notwendigen Attribute für die Steuerung der Zugriffsrechte;
- Definition der Prozesse rund um das Management der Patienteneinwilligungen über Gemeinschaftsgrenzen hinweg;
- Definition der Prozesse bei Eröffnung oder Schliessung eines EPD.

Offene Punkte

Bei der Erarbeitung dieser Empfehlungen sind offene Punkte aufgetaucht, bei denen entweder noch kein Konsens erzielt werden konnte oder die vertiefter analysiert werden müssen:

- Frage: Wie kann sichergestellt werden, dass der Patient einer Gruppe von Gesundheitsfachpersonen ein Zugriffsrecht erteilen kann ohne jede Veränderung der Zusammensetzung der Gruppe bei seinen Zugriffsrechten mitverwalten zu müssen?
- Frage: Wie kann sichergestellt werden, dass eine Gesundheitsfachperson schnell und einfach im HPI registriert werden kann, damit der Patient seine Zugriffsrechte vergeben kann?
- Frage: Wie kann sichergestellt werden, dass der HOI einfach und sicher aktuell gehalten wird durch die anmeldenden Stellen? Welche Prozesse wären dafür notwendig und sind diese heute umsetzbar?
- Frage: Soll das Schreibrecht für Gesundheitsfachpersonen ohne Leserecht als Grundeinstellung oder Option für den Patienten gelten?
- Frage: Müssen angebotene Voreinstellungen einer Qualitätsüberprüfung unterliegen, also sind sie zertifizierungswürdig?
- Frage: Wie kann die Stellvertreterregelung konkret umgesetzt werden, zum Beispiel: Wie bekommt eine Mutter den Zugriff auf das EPD ihres unmündigen Kindes?

- Analyse: Wie können die heutigen Mechanismen der Zugriffsberechtigung im Umfeld von Spitälern mit den Erfordernissen an die Zugriffssteuerung des EPD-Systems abgeglichen werden?
- Analyse: Wie muss der "Informed Consent" ausgestaltet sein, damit er einerseits umfassend und andererseits für alle Beteiligten möglichst einfach handhabbar ist?
- Analyse: Wie sind die hohen Echtzeit-Anforderungen an die Zugriffsteuerung technisch umsetzbar, zum Beispiel Auswertung der aktuellen Rechtematrix oder Aktualität des HPI und HOI?