Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Formular für Stellungnahme zur Anhörung Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG

Stellungnahme von

Name / Kanton / Firma / Organisation	: Interessengemeinschaft eHealth
Abkürzung der Firma / Organisation	: IG eHealth
Adresse, Ort	: Amthausgasse 18, 3011 Bern
Kontaktpersonen	: Walter Stüdeli, Antoinette Feh Widmer
Telefon	: 031 560 00 24
E-Mail	: walter.stuedeli@ig-ehealth.ch; antoinette.feh@ig-ehealth.ch
Datum	: 29. Juni 2016

Hinweise

1. Bitte dieses Deckblatt mit Ihren Angaben ausfüllen.
2. Bitte für jede Verordnung das entsprechende Formular verwenden.
3. Pro Artikel der Verordnung eine eigene Zeile verwenden
4. Ihre elektronische Stellungnahme senden Sie bitte als Word-Dokument bis am **29. Juni 2016** an eHealth@bag.admin.ch

1 Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG

Allgemeine Bemerkungen zu den Erlasstexten

Die IG eHealth begrüsst den Verordnungsentwurf im Grundsatz und bedankt sich beim BAG, dass die Verordnungen in kurzer Zeit erarbeitet wurden.
Wir sind uns bewusst, dass die Thematik äusserst komplex und schwierig ist. Eine Balance zwischen technischer Sicherheit und Praktikabilität und Anwenderfreundlichkeit zu finden, ist ein Spagat, der allerdings nur teilweise gelungen ist. Die IG eHealth ist der Meinung, dass die Regelungstiefe zu hoch ist, worunter die Umsetzung in der Praxis behindert werden könnte. Aus der Sicht der Industrie wurde die Benutzerfreundlichkeit klar der Sicherheit untergeordnet, was sich unserer Ansicht nach schlecht auf die Verbreitung des elektronischen Patientendossiers auswirkt. Die IG eHealth begrüsst grundsätzlich hohe Sicherheitsanforderungen im Sinn einer vertrauensbildenden Massnahme. Allerdings befürchtet Die IG eHealth, dass aufgrund der äusserst hohen Sicherheitsanforderungen die Benutzerfreundlichkeit extrem leidet, die Kosten für Identifikationsmittel in die Höhe getrieben werden und dies dazu führt, dass weder Leistungserbringer noch Patienten das elektronische Patientendossier tatsächlich nutzen werden. Im Weiteren kommt hinzu, dass mit diesen hohen Anforderungen die meisten stationären Leistungserbringer und deren Organisationen zwei Identifikationsmittel einsetzen müssen weil die kantonalen Bestimmungen nicht so restriktiv wie die nun getroffenen Bestimmungen im EPDG sind.
Aus unserer Sicht sollten folgende grundsätzliche Punkte angepasst werden:

1) Die im Zweckartikel genannte Förderung der Gesundheitskompetenz wird mit keinem Wort erwähnt. Das elektronische Patientendossier (EPD) ist auch ein Gesundheitsdossier, in dem Bürgerinnen und Bürger Daten einstellen können. Das Einstellen von Daten durch den Patienten wird in der Verordnung nicht erwähnt. Mittels mHealth-Tools werden heute schon unzählige Daten erfasst. Das sinnvolle Verwalten dieser Informationen ist ein Bedürfnis. Werden diese ins Dossier eingefügt, können sie von medizinischer Relevanz sein. Es braucht unbedingt Massnahmen zur Bürgerkommunikation über Gesundheitsportale und den Zugang zu den EPDs. Hinzu kommt, dass das Hochladen von Daten durch Patienten im Ausführungsrecht schlicht vergessen ging.
2) Oft wird in den Erlasstexten nicht der Prozess beschrieben, das heisst, welche Aufgaben gelöst werden sollen, sondern das „wie“ – also wie die Umsetzung erfolgen soll. So wird beispielsweise die technische Umsetzung detailliert vorgeschrieben. Diese starre Vorgabe widerspricht der Schnelllebigkeit der Technologie. Ein Anpassungsprozess ist nicht beschrieben, es ist nicht klar an wen Anpassungsbegehren zu richten sind, wer darüber entscheidet und bis wann diese einzuführen sind. Technologische und semantische Standards und konzeptionelle Schwächen werden damit eingefroren und der Einsatz neuer Technologien wird erschwert oder gar verhindert. Dies kommt einer ungewollten Überregulierung gleich, die unbedingt verhindert werden muss. Die IG eHealth fordert, dass die Erlasstexte durch einen Prozessbeschrieb ergänzt werden. Dieser soll aufzeigen, wie Änderungen unter Einhaltung welcher Fristen aufgenommen, von wem angenommen und bis wann umgesetzt werden müssen (gibt es ein Antragsrecht oder anfechtbare Verfügungen?). So sollen z.B. technische und semantische Standards nicht in Anhängen mit fixen Ausgaben aufgeführt werden. Zweckmässiger wäre es, die Anbieter von Lösungen für zertifizierte Gemeinschaften als delegierte Vertreter der zertifizierten Gemeinschaft im Sinne eines Change Management Boards die Entscheide fällen zu lassen. Die Entscheide müssen mit einer 2/3 Mehrheit oder einstimmig getroffen werden. Müssen Standards erarbeitet werden, so kann diese Aufgabe an bestehende Standardisierungsorgane wie IHE Suisse oder HL7 Benutzergruppe delegiert wer-

den. Somit wäre es möglich, neue Vorgaben direkt als verbindlich zu erklären. Der gewählte Weg über die Verordnungsanhänge ist zu schwerfällig, es fehlt langfristig die technische Fachkompetenz in der Verwaltung. Jede Änderung bedarf eines langwierigen Prozesses mit internen und externen Konsultationsverfahren.

3) Ein Bestandteil des EPDG ist die Patientenidentifikation und den dafür verwendeten Identifikationsschlüssel. Gemäss den Verordnungen kommen internationale Standards zum Zug, auf schweizerische Eigenentwicklungen wird wo immer möglich verzichtet. Diesen Grundsatz unterstützen wir. Wir schlagen vor, im Rahmen der gesetzlichen Möglichkeiten auch für die Patientenidentifikation auf internationale Identifikationsstandards zu setzen (z.B. GS1) und auf eine proprietäre Umsetzung zu verzichten. Wichtig ist es auch, eine Regelung zu finden wie Asylsuchende, Botschaftsvertreter und Mitarbeiter internationaler Organisationen (WHO, CERN etc.) eine Patientenidentifikationsnummer (PID) erhalten auch wenn diese nicht bei der ZAS geführt sind (Die genannten Personengruppen erhalten keine AHVN13, obwohl sie in der Schweiz wohnhaft sind.).
4) Für die Patienten dürfen systembedingte Strukturen keine Rolle spielen. Unabhängig davon, über wie viele Repositories das virtuelle Dossier verteilt ist, werden die Patienten das System als eine Einheit verstehen. Scheidet nun ein Leistungserbringer aus einer Gemeinschaft aus, dürfen die Patienten erwarten, dass ihre im elektronischen Patientendossier eingestellten Daten in einem Repository der Gemeinschaft verfügbar bleiben.
5) TOZ: Im Anhang 2: Technische und Organisatorische Zertifizierungsvoraussetzungen (TOZ) fehlt eine klare Definition der Systemgrenzen. Dies führt dazu, dass an verschiedenen Stellen im Dokument nicht klar ist, wie die entsprechenden Vorschriften auszulegen sind. Im Weiteren ist auch nicht klar, wie weit in den Organisationen die Zertifizierung gehen soll, welche Kosten für die Teilnehmer im System für die Umsetzung und die Zertifizierung der Lösung entstehen.
6) Zugriff: Der Grundsatz, dass jeder Zugriff auf Daten immer zuerst vom Patienten freigegeben werden muss, ist nicht praktikabel. Speziell weil der Patient nicht in der Lage ist, eine Freigabe zu deklarieren, die für alle Gesundheitsfachpersonen (GFP) gilt (die Gruppendefinition schliesst das aus). Die Idee des Genfer Gesetzes, dass alle Daten auf der Vertraulichkeitsstufe "nützliche Daten" für alle Teilnehmer im System grundsätzlich zugreifbar sind, sollte nochmals geprüft werden. Ein mündiger Patient kann durchaus den Wunsch haben, dass Informationen zu seinen Allergien oder andere für seine Gesundheit essentielle Angaben durch alle GFP eingesehen werden können ohne, dass er gleich alle seine medizinischen Daten zugreifbar machen muss.
7) Anforderungen, die mit dem Konzept des EPDs nicht vereinbar sind: Die IG eHealth hat verschiedene Anforderungen identifiziert, die unserer Meinung nach dem Grundkonzept sowie dem Zweck und der Philosophie des EPDG widersprechen. Zum Beispiel müssen die Daten eines Leistungserbringers gelöscht werden, wenn er die Gemeinschaft verlässt (TOZ 1.1.3.2). Damit werden wichtige Daten für eine bessere Behandlung des Patienten unwiderruflich unzugänglich.
8) Export und Import von medizinischen Dokumenten: Der Export und Wiederimport von medizinischen Dokumenten ist unsinnig, da die Sicherheit des Systems sowie die Integrität der Daten gefährdet werden. Um Daten über eine längere Dauer vom Zugriff der Gesundheitsfachpersonen zu schützen wurde die Vertraulichkeitsstufe „geheime Daten“ geschaffen. Der Patient kann Daten so vor Zugriffen schützen, ohne diese aus dem EPD zu entfernen.
9) Die IG eHealth weist darauf hin, dass sich das Ausführungsrecht einzig über die Frage der Anschubfinanzierung äussert. Der gewählte Prozess einer chronologischen Vergabe der Mittel ist unfair und aus versorgungspolitischen Überlegungen ungeeignet. Die zentrale Frage der Abgeltung des Führens, Pflegens und Aktualisierens eines Dossiers bleibt unbeantwortet. Im Rahmen von DRGs wird es Abgeltungsmöglichkeiten geben, im ambulanten Sektor fehlen spezifische Tarife. Denkbar ist es, dass Ärztinnen und Ärzte für die Pflege des Dossiers die Tarifposition "in Abwesenheit des Patienten" anwenden. Diese Punkte müssen aber an anderer Stelle geklärt werden.
10) In den Empfehlungen von eHealth Suisse sowie der Botschaft zum EDPG war der Zugriff auf Patientendaten auch mittels eines externen Zugangspor-

tals vorgesehen. In den aktuellen Verordnungen ist die Zertifizierung eines externen Zugangsportals aber nicht mehr enthalten. Die IG eHealth ist der Meinung, dass dies für die Entwicklung von eHealth in der Schweiz nicht förderlich ist und innovative Use Cases im Bereich mHealth, Patient Empowerment und allgemeine Innovationen im Gesundheitswesen gebremst werden. Ein „leichtgewichtiger“ Zugang zum EPDG fehlt somit bspw. für Gemeinschaften, welche nicht als Stammgemeinschaft fungieren wollen. Es ist zu prüfen, weshalb in den aktuellen Verordnungen keine externen Zugangsportale mehr vorgesehen sind.
Allgemeine Bemerkungen zu den Erläuterungen

2 BR: Verordnung über die Finanzhilfen für das elektronische Patientendossier EPDFV

Allgemeine Bemerkungen

Die IG eHealth weist darauf hin, dass sich das Ausführungsrecht einzig über die Frage der Anschubfinanzierung äussert. Der gewählte Prozess einer chronologischen Vergabe der Mittel ist unfair und aus versorgungspolitischen Überlegungen ungeeignet. Die zentrale Frage der Abgeltung des Führens, Pflegens und Aktualisierens eines Dossiers bleibt unbeantwortet. Im Rahmen von DRGs wird es Abgeltungsmöglichkeiten geben, im ambulanten Sektor fehlen spezifische Tarife. Denkbar ist es, dass Ärztinnen und Ärzte für die Pflege des Dossiers die Tarifposition "in Abwesenheit des Patienten" anwenden. Diese Punkte müssen aber an anderer Stelle geklärt werden.

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art. 2	Die IG eHealth erachtet es als nicht zielführend, die Stamm-/Gemeinschaften auf zwei pro Kanton zu beschränken. Mit dieser Beschränkung werden bevölkerungsreiche Kantone und allenfalls überkantonale Versorgungsregionen benachteiligt. Zudem verhindert eine Limitierung der Stamm-/Gemeinschaften aus Sicht der Industrie die faire Abbildung von Stamm-/Gemeinschaften.	Die IG eHealth empfiehlt die Beschränkung von zwei Stamm-/Gemeinschaften pro Kanton aufzuheben. Dafür sollte in Art. 2 EPDFV eine Minimalgrösse für Stamm-/Gemeinschaften vorgegeben werden. So sollte eine Stamm-/Gemeinschaft nachweisen müssen, dass sie innerhalb ihres Einzugsgebiets und den darin tätigen Gesundheitsfachpersonen eine Anzahl von mindestens 200‘000 Patienten erreicht (200‘000 individuell abgerechnete Patienten in den letzten zwölf Monaten).
Art. 3 Abs. 1	Die IG eHealth erachtet First come, frist served (Chronologie) als Zuschlagskriterium für die Vergabe von Finanzhilfen als ungeeignet.	Für die IG eHealth ist es zentral, dass bereits vor Beginn der Vergabe der Finanzhilfen eine für alle Systemteilnehmer einsehbare Prioritätenliste vom BAG zur Verfügung gestellt wird, nach welcher die Vergaben erfolgen. Die IG eHealth würde es begrüssen, wenn die Prioritätenliste Zuschlagskriterien nennt, die Anreize im Umgang mit dem elektronischen Patientendossier setzen. Gesuchsteller, die ein umfassendes Konzept zur Einführung des elektronischen Patientendossiers beim BAG einreichen, sollen bevorzugt von den Finanzhilfen des Bundes profitieren. Mögliche Anreize sind aus Sicht der IG eHealth: - Konzept zur langfristigen Bewirtschaftung der elektronischen Patientendossiers - Stand der integrierten Versorgung im Kanton und Massnahmen für den Ausbau

		- Vorweisen eines Gesamtversorgungskonzepts, inkl. Einbindung der ambulanten Leistungserbringer bzw. Gesundheitsfachpersonen
Art. 3 Abs. 2	Finanzhilfen werden gemäss dem Verordnungsentwurf nur gewährt, wenn der Kanton in dem die Stamm-/Gemeinschaft ihren Sitz hat, eine positive Stellungnahme abgibt. Private Stamm-/Gemeinschaften müssen dem Kanton gegenüber ihre Geschäftsmodelle offen legen. Der Kanton übernimmt damit aus der Sicht der Industrie eine Mehrfachrolle: er verfasst Stellungnahmen, entscheidet über die Mitfinanzierung und reguliert die Versorgung. Die IG eHealth erachtet diese Mehrfachrolle der Kantone als problematisch. Das Einsichtrecht der Kantone muss eingeschränkt werden, falls sich diese finanziell nicht an der Trägerschaft beteiligen. Ansonsten müssen gegenüber den Kantonen Geschäftsgeheimisse wie Finanzierungs- und Ertragsmechanismen bekannt gemacht werden, welche den Kanton als Anbieter und direkten Konkurrenten privater Anbieter bevorteilen.	Das BAG muss gemäss Art 23 Abs. 1 EPDG vor der Gewährung von Finanzhilfen die unmittelbar betroffenen Kantone anfragen. Unmittelbar betroffen sind die Kantone nur dann, wenn sie Teil der mitfinanzierenden Trägerschaft sind. Ohne direkte finanzielle Beteiligung der Kantone sind auf Auskunftsvorschriften der Gemeinschaften zu verzichten oder diese sind auf ein absolutes Minimum zu begrenzen (exklusive Finanzierungs- und Ertragsmechanismen).
Art. 4 Abs. 2 lit. b	Bundesseitige Finanzhilfen werden ausschliesslich bei Investitionen geleistet. Finanzielle Beiträge an „Software as a Service“-Modelle sieht der vorliegende Erlassentwurf nicht vor. Dieser Umstand veranlasst die Stamm-/Gemeinschaften eigene IT-Infrastrukturen aufzubauen (Investitionsgeschäft), statt Infrastrukturen zu teilen (Miet-/ Service Modelle).	Die IG eHealth schlägt vor, Art. 4 Abs. 2 lit. b folgendermassen zu ergänzen: […] notwendigen Informatikinfrastruktur **oder Informatikdienstleistungen**,
Art. 5	Die Industrie ist der Meinung, dass sich die Finanzierung viel stärker an den potentiellen Patienten im Einzugsgebiet einer Stammgemeinschaft orientieren sollte. Eine Limitierung der variablen Komponente des Höchstbetrags auf CHF 1.5 Mio. erachtet die IG eHealth als nicht sinnvoll.	Aus Sicht der IG eHealth wäre es wünschenswert, die Limitierung der variablen Komponente nach oben aufzuheben, da die Anzahl Einwohner der Schweiz abschliessend bekannt ist. Es obliegt dem BAG bei sich überschneidenden Stammgemeinschaften zu beurteilen, bei welcher Stammgemeinschaft der variable Betrag von CHF 2.- für ein Patient angerechnet werden soll. Es gilt hierbei folgende Prioritäten absteigend zu berücksichtigen: - Geografische Nähe des Patienten zur Versorgungseinrichtung - Bei vergleichbarer Nähe wird der Patient der kleineren Stammgemeinschaft zugerechnet.

Art. 7	Siehe Kommentar zu Art. 3 Abs. 1	Siehe Vorschläge zu Art. 3 Abs. 1
Art. 11 Abs. 2	Der vorliegende Erlassentwurf sieht ausschliesslich die Vergabe von Finanzhilfen an Stamm-/Gemeinschaften vor, die einen ausreichenden Beitrag an die Gesundheitsversorgung der Schweiz leisten. Dies obwohl sich regionale Stamm-/Gemeinschaften entwickeln können. Aus Sicht der Industrie resultiert daraus eine Benachteiligung von regionalen, überkantonalen Stamm-/Gemeinschaften.	Die IG eHealth schlägt vor, den vorliegenden Erlassentwurf mit einer zusätzlichen Regelung zur Finanzierung von regionalen, überkantonalen Stamm-/Gemeinschaften zu ergänzen.

Bemerkungen zu den Erläuterungen		
Seite / Artikel	**Kommentar**	**Änderungsantrag**

3 BR: Verordnung über das elektronische Patientendossier EPDV

Allgemeine Bemerkungen

Die IG eHealth stellt fest, dass die im Erlasstext genannten Begriffe und Definitionen inkonsistent verwendet werden. So ist beispielsweise der Begriff „Daten“ nicht abschliessend definiert. Dies führt aus der Sicht der Industrie dazu, dass sowohl Leistungserbringer als auch Patienten nicht wissen, wovon die Rede ist: Sind Daten ein Logeintrag, ein Recht, ein medizinischer Wert, ein Dokument oder eine Prozessinformation?
Die im Erlasstext verwendeten Begriffe und Definitionen müssen unbedingt präzisiert werden. Beispielsweise kann der Begriff „Daten“ so definiert werden, dass darunter Dokumente gemeint sind, die von Gesundheitsfachpersonen im elektronischen Patientendossier abgespeichert werden. Weiter sind die Begriffe „löschen“, „informieren“ in den Erläuterungen zum Erlasstext auszuführen.

Grundsätzlich ist aus den Erlasstexten eine Tendenz zur Überregulierung ersichtlich. Das EPDG beschreibt ein starres System. Die technische Umsetzung wird in weiten Teilen vom Eidgenössischen Departement des Innern (EDI) vorgegeben: Absolute Werte als Vorschriften über Speicherkapazität oder Technologien sind nicht in das Ausführungsrecht zu schreiben. In den Erlasstexten fehlt jedoch die Beschreibung eines Anpassungsprozesses für das System. Wie können Anpassungsprozesse vorgenommen und garantiert werden? Gibt es ein Antragsrecht? Für wen? Gibt es anfechtbare Verfügungen? Wer entscheidet über Anträge und innerhalb welcher Fristen sind diese für alle Teilnehmer verbindlich?
Insofern werden konzeptionelle Fehler im System durch die vorliegenden Erlasstexte eingefroren und neue Technologien ausgeschlossen. Aus der Sicht der IG eHealth muss das Ausführungsrecht unbedingt ein lernendes System beschreiben, das innovationsgetrieben weiter entwickelt werden kann. Namentlich sollten technische und semantische Standards in fixen Ausgaben nicht in Verordnungsanhänge aufgenommen werden. Zweckmässiger wäre es, die Anbieter von Lösungen für zertifizierte Gemeinschaften als delegierte Vertreter der zertifizierten Gemeinschaft im Sinne eines Change Management Boards die Entscheide fällen zu lassen. Die Entscheide müssen mit einer 2/3 Mehrheit oder einstimmig getroffen werden. Müssen Standards erarbeitet werden, so kann diese Aufgabe an bestehende Standardisierungsorgane wie IHE Suisse oder HL7 Benutzergruppe delegiert werden. Somit wäre es möglich, neue Vorgaben direkt als verbindlich zu erklären. Der gewählte Weg über die Verordnungsanhänge ist zu schwerfällig, es fehlt langfristig die technische Fachkompetenz in der Verwaltung. Jede Änderung bedarf eines langwierigen Prozesses mit internen und externen Konsultationsverfahren.

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art. 1	Der Begriff Daten muss definiert werden. Es ist klar zu stellen, dass nur bis auf Stufe Dokument Berechtigungen durchgesetzt werden. Rechte können nicht bis auf ein einzelnes Datum innerhalb eines Dokuments angewendet werden. Die IG eHealth hat die von eHealth Suisse empfohlenen	Art 1 Abs. 1 Die Patientin oder der Patient kann die Daten die in einem Dokument zusammengefasst sind einer der folgenden vier Vertraulichkeitsstufen zuordnen: …. Art 1 Abs. 1 neuer Buchstabe: Regelung wie mit sensiblen administrati-

	fünf Vertraulichkeitsstufen unterstützt. Mit der Streichung der Kategorie administrative Daten besteht nun die Lücke wie ein Zugriff auf schützenswerte Informationen im Master Patient Index wie z.B. der Religionszugehörigkeit zu regeln sind. Im Weiteren ist es denkbar, dass in Gemeinschaften die z.B. nur Diabetiker behandeln, bereits der Zugang zu den Administrativdaten (Demografische Daten im MPI) dieser Gemeinschaft sensiblen Charakter haben können. Die IG eHealth kann auch die 4 gewählten Stufen unterstützen, es muss allerdings geregelt werden wie mit mit sensiblen Daten aus dem MPI umgegangen werden muss. Der hier beschriebene Mechanismus kann so nicht umgesetzt werden. Dies würde erfordern, dass der Patient jedes neu publizierte Dokument zuerst prüfen muss, damit er oder sie die Vertraulichkeitsstufe korrekt setzen kann.	ven Daten umgegangen werden soll. Änderung Abs. 2: Neu eingestellte Daten werden, sofern die GFP nichts anderes zuweist, mit der Vertraulichkeitsstufe „medizinische Daten“ gespeichert.
Art. 2	Abs. 4 und 5: In der Grundeinstellung wird der Patient über alle Gruppenänderungen, aber nicht über Notfallzugriffe informiert. Die IG eHealth ist der Meinung, dass diese Grundeinstellung zu einer verwirrenden Informationsflut gegenüber dem Patienten und einer persönlichkeitsverletzenden Transparenz der Versetzung von Gesundheitsfachpersonen führt. Der Patient erhält viele nicht zweckmässige Mutationsmeldungen. Abs. 5: Wichtige Informationen sollten mit der Vertraulichkeit „nützliche Daten“ für alle GFP abrufbar sein. Dies entspricht auch der Standardeinstellung gemäss Abs. 2. Der Patient kann Daten wie Allergien, Unverträglichkeiten, Impfstatus und weitere wichtige Informationen vorgängig als nützliche Daten kennzeichnen. Medizinische oder sensible Daten (Option) sollten nur einer Ärztin oder einem Arzt in einem medizinischen Notfall zugänglich gemacht werden. Als kompensierende Massnahme zum Wegfall	Abs. 4 unverändert, in Art. 3 werden jedoch die Optionen angepasst. Abs. 5: In medizinischen Notfallsituationen können Ärzte auf die Vertraulichkeitsstufen „medizinische Daten“ zugreifen. Sie müssen einen solchen Zugriff vorgängig durch eine Willensbekundung bestätigen. Die Willens-

	der Begründung sind der Patient und sein Hausarzt bei einem Notfallzugriff zwingend zu informieren. (siehe auch Vorschläge zu Art 17) Die Stammgemeinschaften und Gemeinschaften sollten standardmässig ermächtig werden, Rechte bei Delegationen weiter zu geben. Der Patient kann dies in den Optionen einschränken.	bekundung muss den Hinweis enthalten, dass der Zugriff nur in einer medizinischen Notfallsituation des Patienten durchgeführt werden darf. Der Patient und sein Hausarzt sind über diesen Notfallzugriff zu informieren. Abs. 6 neu: Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft sind ermächtigt, im Namen der Patientin oder des Patienten Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen; dabei können diese höchstens die Zugriffsrechte zuweisen, die sie selber besitzen.
Art. 3	lit. a: Der IG eHealth scheint eine feste Dauer von 6 Monaten zu starr. Es kann sein, dass einer GFP das Recht nur für eine Konsultation (einige Minuten bis Stunden) erteilt werden soll. lit. e: Der Patient wird bei jeder Mutation zwingend informiert. Dies kann bei chronisch Kranken oder komplex kranken Patienten zu einer grossen, unseres Erachtens nicht zweckmässigen Informationsflut führen. lit. f: Diese Anforderung steht im direkten Widerspruch zur Verständlichkeit und zur einfachen Nachvollziehbarkeit der Lösung. Entweder vertraut ein Patient der Organisation und vertraut darauf, dass sich die Organisation auch selber organisieren kann. Ansonsten vertraut er Individuen. Im Weiteren müssten dann pro Patient individuell zusammengesetzte Gruppen für die Berechtigung gebildet werden, was die Komplexität und Evaluation der Zugriffe ins unermessliche ausweiten würde.	Abs. 1 lit. a ändern: Festlegen, dass die Zugriffsrechte nach Art. 2 Abs. 1 nach maximal sechs Monaten erlöschen. lit. e ändern: Kann jederzeit die aktuelle Zusammensetzung einer Gruppe von GFP abrufen. lit. f ändern: Kann festlegen, dass keine Zugriffsrechte an Gruppen erteilt werden.

	lit. g: Diese Regelung ist gut, greift jedoch zu kurz. Was geschieht beim Verlust der Handlungsfähigkeit? Verliert dann der Patient seine Rechte auf Optionen? Erhält sein Vertreter alle Rechte oder wird das Patientendossier gelöscht? lit. h: Die Weitergabe von Rechten bei Delegationen sollte eine Standardeinstellung sein. Der Patient soll dies optional aber einschränken können.	lit. g ergänzen: Wie ist bei Verlust der Handlungsfähigkeit zu verfahren? lit. h ändern: Kann die Weitergabe von Rechten an weitere GFP seiner Stammgemeinschaft verbieten oder auf die Weitergabe an maximal eine weitere GFP oder Gruppe einschränken.
Art. 4	Abs. 1: Es dürfte zweckmässig sein, für die Patientenidentifikation einen internationalen Standard einzusetzen wie den GS1-GSRN (Global Service Relation Number). Damit könnte auf eine Schweiz spezifische Lösung verzichtet werden. Die Einbindung von Ausländerinnen und Ausländern ins System des elektronischen Patientendossiers wäre wesentlich einfacher.	Änderung Abs. 1: Die Patientenidentifikationsnummer ist nach internationalen Standards für Personenidentifikationsnummern aufgebaut. Diese darf für eine bestimmte, im Register der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) nach Art. 71 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG) verzeichnete Person verwendet werden, jedoch keinerlei Rückschlüsse auf diese Person zulassen.
Art 5.	Abs. 1: Die Patientenidentifikationsnummer darf nur für eine bestimmte, im Register der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) verzeichnete Person (obligatorisch Versicherte Person nach Art. 1 Abs. 1 AHVG) verwendet werden. Das heisst, es können nur Patientenidentifikationsnummern für Personen generiert werden, die eine AHVN13 besitzen, also AHV versichert sind. Vielen Ausländern, Reisenden, Grenzgängern, Mitarbeitenden in Botschaften, Konsulaten sowie bei internationalen Organisationen ist es mit dieser Regelung nicht möglich, ein elektronisches Patientendossier zu eröffnen, weil sie nicht in der Identifikationsdatenbank der zentralen Ausgleichsstelle erfasst sind und auch nicht in diesem Register ohne Änderung des Art. 71 Abs. 4 lit. a resp. Art. 1 AHVG erfasst werden dürfen.	Änderung Abs. 1: Die Patientenidentifikationsnummer wird auf Antrag einer Stammgemeinschaft durch die ZAS vergeben. Die ZAS stellt sicher, dass auch nicht obligatorisch Versicherte nach Art. 1 AHVG im zentralen Versichertenregister ohne AHVN13 geführt werden können und das die Stammgemeinschaften für diese Personen eine Patientenidentifikationsnummer beantragen dürfen.
Art. 8 / Art. 40	Gesundheitsfachpersonen können Hilfspersonen für die	Änderung Abs. 1: Gemeinschaften müssen die ihnen angehörenden Ge-

	Bearbeitung von Daten des elektronischen Patientendossiers einsetzen. Allerdings werden Hilfspersonen gemäss den Erläuterungen zur EPDV nicht im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Art. 40 geführt. Für die IG eHealth stellt sich die Frage, wie der Gesetzgeber nun sicherstellen will, dass der Patient die Identitäten der Hilfspersonen auch über die verschiedenen Stamm-/Gemeinschaften hinweg kennt und sieht, wem er den Zugriff auf seine Daten erteilt? Der Erlasstext unterlässt es, zu definieren, wie Hilfspersonen gemeinschaftsübergreifend identifiziert und damit für den Patienten datenschutzkonform erkennbar gemacht werden können.	sundheitseinrichtungen, Gesundheitsfachpersonen, **Hilfspersonen** und Gruppen von Gesundheitsfachpersonen verwalten. …
Art. 9	Abs. 1: Wie bereits in den allgemeinen Anmerkungen aufgeführt, sind die in Art. 9 verwendeten Begriffe und Definitionen unpräzise. Aus der Sicht der Industrie ist es unklar, was die Begriffe „Datenspeicherung“, „Löschung“, „Vernichtung“ und „Aufbewahrungsdauer“ bedeuten. Einerseits wird eine strikte Trennung von Primär- und Sekundärdaten verlangt, die eine physische Trennung der Daten vermuten lässt, andererseits ist eine Verlinkung und einmalige Speicherung der Daten erlaubt. Für die Anbieter ist eine einheitliche Definition der Begrifflichkeiten jedoch zentral. Nur so kann die praktische Umsetzung gelingen. Wir weisen an dieser Stelle darauf hin, dass die international verwendeten IHE Profile das Löschen in eigenen und fremden Gemeinschaften nicht unterstützen. Daten können nur „unterdrückt“ werden, d.h. für alle Benutzer nicht mehr zur Anzeige gebracht werden. Der medizinische Wert des EPD liegt in der Langzeitbetrachtung der medizinischen Daten eines Patienten. Es ist daher unsinnig Daten nach zehn Jahren zu löschen. Der Patient kann jedoch daran erinnert werden, dass Daten schon lange nicht mehr verwendet wurden.	Art 9. Abs. 1 neuer erster Buchstabe: Daten im elektronischen Patientendossier einen, von den von der Gesundheitsfachperson erfassten Primärdaten, unabhängigen Lebenszyklus haben. Änderung Abs. 1 lit. a: dass der Patient darüber informiert wird, wenn von einer Gesundheitsfachpersonen im elektronischen Patientendossier erfasste Daten zehn Jahre nicht mehr abgerufen wurden.

	Abs. 2: Die folgende Formulierung ist unklar: Sie haben auf Verlangen der Patientin oder des Patienten. Auf wen bezieht sich das Sie – auf Gesundheitsfachpersonen?	Änderung Abs. 2: Gemeinschaften haben auf Verlangen […]
	Abs. 2 lit. a: Es erscheint der IG eHealth organisatorisch unlösbar, dass der Patient individuell der Gemeinschaft eindeutig mitteilen kann, welche zukünftigen Daten nicht durch eine GFP im Dossier gespeichert werden dürfen.	Änderung Abs. 2 lit. a: alle neuen Dokumente ab einem vom Patienten bestimmten Zeitpunkt mit der Vertraulichkeitsstufe „geheime Daten“ oder „sensible Daten“ in seinem elektronischen Patientendossier zu speichern.
	Abs. 2 lit. b: Da nicht mehr durch die Gemeinschaft gelöscht wird, entfällt dieser Punkt.	Abs. 2 lit. b ist aufgrund Abs. 1 lit. a neu zu streichen.
	Abs. 2 lit. c: Was ist der Unterschied zwischen Löschen und Vernichten? Wir weisen darauf hin, dass der Patient hier der Gemeinschaft einigen Aufwand auferlegen kann. Weiter kann es sein, dass so Daten unwiderruflich gelöscht werden, da die Primärdaten evtl. auch bereits aufgrund kantonaler Bestimmungen gelöscht werden mussten.	Abs. 2 lit. c: bestimmte, auf diese oder diesen bezogene Daten aus dem elektronischen Patientendossier zu **löschen**.
	Es ist unklar, was mit dem Wort „ausschliesslich“ gemeint ist, da es als doppelte Ablage interpretiert werden könnte. Dies wäre nicht zielführend, da die Kosten verdoppelt würden und das Handling in der Praxis unrealistisch und stark fehleranfällig wäre.	c. Daten des elektronischen Patientendossiers nur in Ablagen gespeichert werden, die ~~ausschliesslich~~ dafür vorgesehen sind.
Art 10.	Die IG eHealth erachtet diese vollumfängliche Delegation der Definition der Zugangsportale für GFP an das EDI an dieser Stelle als sehr umfassend. Die minimalen Anforderungen an das Zugangsportal sind nach Meinung der IG eHealth zu definieren, damit ein einheitliches und interoperables Funktionieren des EPD gewährleistet ist.	Art. 10 neu Abs. 1: Gemeinschaften müssen ein Zugangsportal für GFP betreiben, welches der GFP ermöglicht mit deren Identifikationsmittel über deren Zugang zum Internet ohne weitere Hilfsmittel einzuloggen und minimal, nicht abschliessend: lit. a: eine Patientin, einen Patienten zu suchen und eindeutig mit seinen demografischen Daten, der Personenidentifikationsnummer, der AHVN13

		oder der Versichertenkartennummer nach Art. 42a KVG zu identifizieren. lit. b: Daten der Behandlung für die Patientin und den Patienten in deren Dossier mit einer definierten Vertraulichkeitsstufe zu laden und nützliche Daten oder weitere Daten nach Art. 2 der Patienten, sofern die Patienten, der Patient der GFP ein Zugriffsrecht erteilt hat, anzuzeigen. lit. c: angezeigte Daten eines Patienten so abrufbar zu machen, dass diese über eine Schnittstelle in das Primärsystem der GFP übernommen werden können. lit. d: erweiterte Zugriffsrechte beim Patienten anzufragen, um die Sicherheit des Patienten bei einer Behandlung zu erhöhen. lit. f: Zugriffe auf ein Patientendossier an eine andere Gesundheitsfachperson oder an eine Hilfsperson delegieren zu können. Abs. 2: Das Zugangsportal muss für Ärztinnen und Ärzte zudem: lit. a: in einem Notfall zusätzlich zu den nützlichen Daten auch medizinische Daten oder sogar sensible Daten des Patienten nach einer Willensbekundung des Notfallzugriffs durch die betreffende Ärztin, den Arzt anzeigen können. lit. b: einer Patientin oder einem Patienten den Status Ärztin, Arzt des Vertrauens (Hausarzt) zu gewähren, um damit Notfallzugriffe auf sein Dossier anzuzeigen. Abs. 3: Das Zugangsportal für Gesundheitsfachpersonen ermöglicht für Stammgemeinschaften zudem: lit. a: neue Patientinnen und Patienten nach deren Einwilligung von Gesundheitsfachpersonen und Hilfspersonen mit deren Identifikationsmittel zu registrieren. lit. b: das Todesdatum einer in dieser Stammgemeinschaft registrierten

		Patientin oder eines Patienten zu erfassen. Das setzen eines Todesdatums führt zu einem temporären Entzug der Zugriffsrechte nach Art. 2 und zu einer Information an den Patienten, seine Vertreter und den Arzt des Vertrauens (Hausarzt).
Art 15.	Es ist sicher zu stellen, dass die Unterzeichnung der Einwilligung auch durch eine elektronische Unterschrift erfolgen kann.	Änderung Art. 15: Die Stammgemeinschaft hat von der Patientin oder dem Patienten die Einwilligung zur Führung eines elektronischen Patientendossiers einzuholen. Diese muss von der Patientin oder vom Patienten nach Art. 14 Abs. 2^{bis} des Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches, Fünfter Teil: Obligationenrecht unterzeichnet sein.
Art 16	Abs. 1 lit. d: Die aktuelle Regelung erlaubt es nur obligatorisch versicherten Personen nach Art 1 AHVG eine Personenidentifikationsnummer zu zuteilen. Ausländern, Reisenden, Grenzgängern, Mitarbeitenden in Botschaften, Konsulaten sowie bei internationalen Organisationen können mit dieser Regelung keine Personenidentifikationsnummern zugeteilt werden, obwohl diese Personengruppen eine namhafte Anzahl Patienten stellen können. Diese Personengruppen können kein EPD haben und sind damit vom System ausgeschlossen, obwohl diese Personen Anrecht auf Sozialleistungen aufgrund der bilateralen Verträge haben. Abs. 1 lit. e: Ist zu offen formuliert, auch die EPDV-EDI gibt keine Informationen zu den verlangten Anforderungen. Der Erlasstext ist so anzupassen das die Anforderungen für einen Wechsel einer Stammgemeinschaft für die Stammgemeinschaften klar sind.	Siehe Änderung in Art.5 Abs. 1. Abs. 1. lit. e ändern: Für einen Wechsel des Patienten in eine andere Stammgemeinschaft alle nötigen Daten, Zugriffsregeln und Logeinträge der neuen Stammgemeinschaft für eine Übernahme zugänglich machen, so dass Zugriffe auf das EPD weiterhin in vergleichbarem Umfang erfolgen können. Das EDI legt den Umfang der Formate der zu transferierenden Daten fest.
Art 17	Die IG eHealth erachtet diese vollumfängliche Delegation der Definition der Zugangsportale für Patientinnen und Patienten an dieser Stelle an das EDI als sehr unpassend. Die minimalen Anforderungen an das Zugangsportal sind nach Meinung der IG eHealth zu definieren, damit ein einheitliches und interoperables Funktionieren des EPD ge-	Art. 17 neu: Stammgemeinschaften müssen ein Zugangsportal für Patientinnen und Patienten betreiben, welches der Patientin, dem Patienten ermöglichen, mit seinem Identifikationsmittel über seinen Internetzugang ohne weitere Hilfsmittel einzuloggen und mindestens, nicht abschliessend:

	währleistet ist.	lit. a: seine im elektronischen Patientendossier selber gespeicherten persönlichen Gesundheitsdaten und gespeicherte Daten der Gesundheitsfachpersonen anzuzeigen und diese über eine Schnittstelle auch herunterladen zu können. lit. b: persönliche Gesundheitsdaten in sein elektronisches Patientendossier hochzuladen. lit. c: an die Patientin oder den Patienten gerichtete Nachrichten (Informationen) vom Patientendossier-System oder von Gesundheitsfachpersonen anzuzeigen. Hierbei kann der Patient über einen unsicheren Kanal auf das Vorliegen von Informationen in seinem Dossier hingewiesen werden. lit. d: Logeinträge des Patientendossier-Systems in für den Patienten lesbarer und verständlicher Sprache benutzerfreundlich anzuzeigen. lit. e: das Erstellen und Löschen von Vertraulichkeitsstufen und Zugriffsrechten auf seine Daten nach Art. 1 und 2 vorzunehmen. lit. f: das An- und Abschalten der Optionen nach Art. 3 zu wählen. lit. g: eine Patientenverfügung nach Art. 371 ZGB zu speichern oder zu widerrufen. lit. h: eine Vertretung nach Art. 378 ZGB zu erfassen oder zu löschen, hierbei muss der Vertreter über ein gültiges Identifikationsmittel verfügen und der Patient einen Auftrag zur Personensorge nach Art 360 Abs. 2 und Art 361 ZGB an den Vertreter erteilen wobei eine elektronische Kopie des handschriftlich verfassten Auftrags ausreichend ist. lit. i: den Zugang zum Patientendossier auf Verlangen des Vertreters eines urteilsunfähigen Patienten bis zur Erlangung dessen Urteilsfähigkeit zu sistieren, sofern ein gesetzlicher Vertreter nach lit. h vorliegt.

		lit. j: die Aufhebung des Dossiers und damit die Löschung der Daten zu beantragen.
Art 20	Die aktuelle Formulierung zur Löschung eines elektronischen Patientendossiers kann dazu führen, dass medizinische Daten des Patienten, ohne diesen zu benachrichtigen, automatisch unwiderruflich gelöscht werden. Da die Daten der Primärsysteme je nach kantonaler Regelung ebenfalls gelöscht werden müssen, kann dies zu einem ungewollten Datenverlust führen. Wie soll die Stammgemeinschaft den Tod feststellen?	Abs. 1: Ein elektronisches Patientendossier wird von der Stammgemeinschaft aufgehoben, wenn Neu lit. anstelle lit. a: nach unbeantwortetem Verstreichen einer Frist von 90 Tagen auf schriftliche Aufhebungsmitteilung an den Patienten, seine Vertreter und seinen Arzt des Vertrauens (Hausarzt); Änderung Abs. 1 lit. c: von einer Gesundheitsfachperson oder Hilfsperson das Todesdatum erfasst wurde und eine Amtsstelle, ein Angehöriger oder ein Vertreter des Patienten der Stammgemeinschaft den Tod des Patienten bescheinigt hat. lit. a-c werden neu zu lit. b-d nummeriert.
Art. 21 Abs. 2	Gemäss dem Erlasstext legt das EDI die zu liefernden Daten fest. Aus der Sicht der IG eHealth sollte dieser Absatz durch die Angabe von Fristen zur Einreichung der zu liefernden Daten ergänzt werden.	Vorschlag für Art 21 Abs. 2: Das EDI legt die zu liefernden Daten sowie die **Fristen für die Einreichung** der zu liefernden Daten gemeinsam mit den betroffenen Kreisen fest.
Art. 22	Die IG eHealth ist der Ansicht, dass die Anforderungen an die Identifikationsmittel sehr hoch sind. Die im Erlasstext genannten Anforderungen gehen so weit, dass die in den Spitälern bereits heute eingeführten Identifikationsmittel für den Zugriff auf das elektronischen Patientendossier in den meisten Fällen ausgeschlossen werden obwohl diese kantonalen Bestimmungen genügen. Damit müssen die Gesundheitsfachpersonen der Leistungserbringer mit neuen Identifikationsmitteln für den Zugriff auf das elektronische Patientendossiers ausgerüstet werden. Für die Industrie wird dadurch einerseits die Attraktivität des elektronischen Patientendossiers für Gesundheitsfachpersonen geschmälert, weil sie für ihre Tätigkeit zwei Logins benötigen. Andererseits stehen die stationären Leistungserbringer vor einer grossen Herausforderung, wenn sie ihr Per-	Die IG eHealth fordert, dass Art. 22 mit einer Übergangsbestimmung ergänzt oder wie folgt angepasst wird: In all jenen stationären Einrichtungen, in welchen die Gesundheitsfachpersonen ein nach kantonalem Recht gültiges Identifikationsmittel für den Zugriff auf Patientendaten einsetzen, kann dieses Identifikationsmittel auch für den Zugriff auf das elektronische Patientendossier verwendet werden.

	sonal mit einem zweiten Identifikationsmittel ausrüsten müssen.	
Art. 25	Gemäss Art. 25 Abs. 2 überprüft der Herausgeber des Identifikationsmittels bei dessen Erneuerung die Identität der antragstellenden Person erneut. Für die IG eHealth ist diese erneute Überprüfung der Identität der antragstellenden Person überflüssig, sofern das Identifikationsmittel zu diesem Zeitpunkt noch gültig ist.	Änderung Abs. 2: Verliert ein Identifikationsmittel seine Gültigkeit, so muss der Herausgeber des Identifikationsmittels für dessen Erneuerung nach Art. 23 die Identität der antragstellenden Person neu überprüfen.
Art. 29	Das EPDG beschreibt ein starres System. Viele technische Vorgaben werden durch das Eidgenössische Departement des Innern (EDI) vorgegeben. Der vorliegende Erlasstext beschreibt allerdings nirgends, wie Anpassungsprozesse vorgenommen und garantiert werden (siehe allgemeine Anmerkungen).	Die IG eHealth schlägt vor, den vorliegenden Erlasstext durch einen neuen Abschnitt „Systemanpassungen“ zu ergänzen.
Neuer Abschnitt Systemanpassungen	Wie in den einleitenden Bemerkungen und unter Art. 29 beschrieben, vermisst die Industrie einen Prozess wie Anpassungen am System wirksam eingeführt werden können. Es besteht das Risiko, dass das EDI die notwendigen Spezialisten zur Prüfung und Ausarbeitung von Anpassungen nicht vorhalten kann. Ein wirksamer Prozess zur Evaluation und Umsetzung von Anpassungen ist aber in diesem komplexen System von essentieller Bedeutung.	Neuer Artikel: Antragsstelle für Systemänderungen: Das EDI betreibt eine Antragsstelle an die Systemänderungen gerichtet werden können. Die Antragsstelle prüft, ob der Änderungsantrag vollständig und von einem berechtigten Antragsteller (Stammgemeinschaft oder Gemeinschaft oder einer deren Delegierten) ist und gruppiert gleichgelagerte Anträge. Die Anträge werden nach deren Dringlichkeit und Datum des Eingangs sowie Relevanz auf das Gesamtsystem priorisiert. Das EDI übergibt diese Anträge dem Gremium zur Prüfung von Änderungen. Zur Umsetzung der vom Gremium verabschiedeten Änderungen erarbeitet das EDI in Zusammenarbeit mit Stammgemeinschaften und Gemeinschaften und der Industrie die rechtlichen, technischen und organisatorischen Umsetzungsvorgaben. Neuer Artikel: Gremium zur Prüfung von Änderungen Das EDI fordert jede zertifizierte Stammgemeinschaft und Gemeinschaft auf, einen Vertreter in ein Änderungsgremium zu delegieren. Die Vertreter müssen über die notwendigen fachlichen Qualifikationen verfügen, um prozessuale, rechtliche und technische Änderungsanträge beurteilen zu können. Weiter ist eine Person von eHealth Suisse, als Vertreter von Bund und Kantonen, ein Vertreter von IHE Suisse sowie ein Vertreter der ICT-Industrie ständiges Mitglied.

		Neuer Artikel: Aufgaben des Gremiums zur Prüfung von Änderungen sind: Die delegierten Vertreter prüfen die Änderungsanliegen auf deren Notwendigkeit und Umsetzbarkeit. Sie setzen fest, in welchem Umfang und in welcher Frist eine Änderung umgesetzt werden muss. Das Gremium muss die Entscheide protokollieren und auf Verlangen Dritten zugänglich machen. Neuer Artikel: Freigabe von Änderungen und deren Umsetzung Jeder Vertreter hat eine Stimme. Abstimmungen gelten mit Zweidrittelmehrheit Zustimmung als angenommen. Änderungen der Zusammensetzung des Gremiums bedürfen der Einstimmigkeit.

Bemerkungen zu den Erläuterungen

Seite / Artikel	Kommentar	Änderungsantrag
Art. 1, Seite 10	Die Begrifflichkeiten "Daten vs. "Dokument" sind zu schärfen: Bisher wurde in der Diskussion davon ausgegangen, dass Autorisierungen entweder auf das ganze Patientendossier oder aber auf einzelne Dokumente im Patientendossier zu beziehen sind. Der Begriff Daten ist aber sehr viel allgemeiner und könnte so interpretiert werden, dass verschiedene Daten in einem Dokument unterschiedlich zu klassifizieren und zu autorisieren sind.	Es ist klarzustellen, dass ein Dokument die kleinste autorisierbare Entität darstellt. Die Anforderungen an die Unabhängigkeit der Daten im Patientendossier versus denselben Daten in Primärsystem sind zu beschreiben, nicht die technische Umsetzung.
Art. 2, Seite 10, 11	In der EPDV steht: „Nimmt die Patientin oder der Patient keine Zuweisung vor, so gilt das Zugriffsrecht „normal“. Das kann so interpretiert werden, dass jeder Behandelnde automatisch das Zugriffsrecht “normal” erhält, wenn der Patient nichts anderes definiert.	Die IG eHealth empfiehlt die eingeführten Begriffe unter Ziff. a-c in Abs. 1 von Art. 2 zu streichen, da diese sowieso in einer 1:1-Beziehung zu den Vertraulichkeitsstufen stehen. Weiter sollte ein Zugriff auf „medizinische Daten“ nur mit einer zusätzlichen Rechtevergabe des Patienten, als nicht automatisch nach eröffnen des Dossiers, möglich sein. In der Grundeinstellung haben die Gesundheitsfachpersonen Zugriff auf demographische und nützliche Daten.
Art 2, Seite 11	„Wie die Informationspflicht umgesetzt wird, ob die Patien-	Die Informationspflicht sollte so definiert werden, dass die Stammge-

	tin oder der Patient z.B. per Brief, Email oder SMS über einen erfolgten Notfallzugriff informiert wird, bleibt den Gemeinschaften überlassen.“ Die Informationspflicht kann nicht delegiert werden, weil nur die Stammgemeinschaft weiss, ob der Patient überhaupt eingewilligt hat, dass Notfallzugriffe zulässig sind. Dies hat auch den Vorteil, dass der Patient beim Eintritt in die Stammgemeinschaft erfährt, wie die Stammgemeinschaft in solchen Fällen informiert, respektive dass der Patient entscheiden kann, wie er informiert werden will. Notfallzugriffe müssen nicht nur an den Patienten, sondern auch an seine Vertreter (des Patienten) und den Arzt des Vertrauens (Hausarzt) gesendet werden.	meinschaft des Patienten diese Verpflichtung hat. Die Stammgemeinschaft darf keine schützenswerten Informationen über unsichere Kanäle dem Patienten senden. Die Informationspflicht gilt als erfüllt, wenn die Stammgemeinschaft dem Patienten über einen unsicheren Kanal z.B. SMS oder Email die Aufforderung zum Einloggen in ein EPD versendet, sodass der Patient danach die vorliegende Informationen auf eine sicher Art und Weise einsehen kann. Verfügt der Patient bereits über einen sicheren Kanal (z.B. verschlüsseltes Email), kann die Information direkt an den Patienten versendet werden. Der Kreis der zu informierenden Personen bei einem Notfall ist zu erweitern, da der Patient in dieser Situation vielleicht nicht mehr urteilsfähig ist und nicht reagieren kann. Vertreter des Patienten und der Arzt des Vertrauens (Hausarzt) sind im Notfall wichtige Kontakte, die es im Notfall ebenfalls zu informieren gilt. Hat der Patient keinen Vertreter und keinen Arzt des Vertrauens definiert, wird nur der Patient informiert.
Art. 3, Seite 13	Beschränkung der Zugriffsrechte auf genau 6 Monate ist nicht genügend.	Ändern: Die Dauer der Zugriffsrechte auf maximal 6 Monate, nicht fix 6 Monate. Es kann sein, dass ein Zugriffsrecht nur für einige Minuten gewährt werden soll.
Art. 3, Seite 13	„Die Patientin oder der Patient hat nach Buchstabe h die Möglichkeit, Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft zu ermächtigen, das ihr erteilte Zugriffsrecht an weitere Gesundheitsfachpersonen weiterzugeben.“ Es ist unklar, ob die Weitergabe von Delegationen gestattet ist oder nicht.	Vorschlag: […] das ihr von Patienten erteilte Zugriffsrecht an weitere Gesundheitsfachpersonen weiterzugeben.“
Art. 8, Seite 14	“Austrittsprozess: Zudem müssen Gemeinschaften beim Austritt einer Gesundheitseinrichtung, die sich keiner anderen Gemeinschaft oder Stammgemeinschaft anschliesst, sicherstellen, dass diejenigen Dokumente gelöscht werden, die von der austretenden Gesundheitseinrichtung in den gemeinschaftsinternen oder eigenen Dokumentenablagen für das elektronische Patientendossier	Der Austritt einer Organisation oder einer Gesundheitsfachperson darf nicht dazu führen, dass Daten aus dem Patientendossier verschwinden. Die Gemeinschaft muss sicherstellen, dass alle Dokumente auch nach dem Austritt einer GFP oder einer Gesundheitseinrichtung weiterhin verfügbar sind.

	bereitgestellt wurden." Die Forderung der Löschung ist mit dem Zweck des Gesetzes nicht vereinbar. Das EPDG ist ein Patienten zentriertes Gesetz. D.h. die eingestellten Dokumente unterliegen der Kontrolle des Patienten. Austreten der Gesundheitseinrichtung Das Löschen der Dokumente einer austretenden Gesundheitseinrichtung widerspricht dem Prinzip der sekundären Datenhaltung, sowie der Grundidee, dass die Datenhoheit beim Patienten liegt.	
Art. 8, Seite 14	Eintrittsprozess: Dazu zählt insbesondere die Verwaltung der Gesundheitsfachpersonen und der Gruppen von Gesundheitsfachpersonen, die in der entsprechenden Gesundheitseinrichtung arbeiten. Die Ausgabe und Verwaltung der Identifikationsmittel zur Authentisierung für Mitarbeiter der Gesundheitseinrichtung wird an dieser Stelle nicht erwähnt. Aus unserer Sicht sollten bestehende Identifikationsmittel und Authentisierungsverfahren in Organisationen die für die Öffentlichkeit Leistungen erbringen und den kantonalen Bestimmungen genügen, auch für den Zugriff auf das EPD ausreichen.	Es ist in die Erläuterung aufzunehmen, dass öffentliche Gesundheitseinrichtungen und private Gesundheitseinrichtungen die öffentliche Versorgungsleistungen erbringen, welche Identifikationsmittel und Authentisierungsverfahren verwenden, die den kantonalen Datenschutzbestimmungen genügen, auch mit diesen Mitteln und Verfahren auf das EPD zugreifen dürfen.
Art. 8, Seite 15	Die Verwendung der Begriffe „Identifikation", „Identifikationsmittel", „Authentisierung", „Authentisierungsmittel" ist irreführend. Insbesondere der Begriff des „Identifikationsmittels" wird häufig falsch verwendet.	Bessere Definition: Authentisierung: Der Prozess der Authentisierung prüft, ob die sich authentisierende Person wirklich Inhaber der behaupteten Identität ist. Diese Prüfung verwendet das der elektronischen Identität zugeordnete Authentisierungsmittel. Beispiele von Authentisierungsmitteln: FMH ID, SuisseID, etc. Identitätsprüfung: Die Identitätsprüfung prüft, ob eine Person Inhaber ei-

		ner Identität ist. Diese Prüfung ist immer Teil des Registrationsprozesses. Sie benötigt ein Identifikationsmittel. Sie assoziiert ein Authentisierungsmittel zur Identität.
Art. 8, Seite 15	Woher sollen die Daten dieser Hilfspersonen kommen? Gibt es eine einheitlich strukturierte Datenbank dafür?	Hilfspersonen sind in das zentrale Register der Gesundheitsfachpersonen aufzunehmen, um zu gewährleisten, dass diese auch gemeinschaftsübergreifend identifizierbar und für den Patienten erkennbar sind.
Art. 9, Seite 16	In technisch begründeten Ausnahmefällen (vgl. Erläuterungen zu Art. 9 Abs. 1 lit. c) liegen die Daten resp. Dokumente nicht in Kopien vor, sondern werden direkt aus den integrierten Ablagen der Primärsysteme abgerufen. Wenn der Austritt einer Gesundheitseinrichtung angepasst wird, dann muss auch hier eine Anpassung vorgenommen werden, weil die Löschung durch die GFP nicht mehr gestattet ist.	Dieser Satz sollte gelöscht werden. Die Ausführungsbestimmungen beschreiben Anforderungen, nicht technische Umsetzungen.
Art. 11, Seite 21	Die folgende Formulierung scheint unglücklich gewählt: Es muss die Komplexität und Grösse der Gemeinschaft, sowie der Umfang der in der Gemeinschaft erfassten Daten und Dokumente des elektronischen Patientendossiers berücksichtigen (vgl. Ziff. 4.2 der TOZ) Das bedeutet, dass eine Gemeinschaft mit 5000 Patienten grundsätzlich weniger sicher sein darf, als eine Gemeinschaft mit 100‘000 Patienten. Da sich aber die Sicherheit eines Systemverbundes über die Sicherheit des schwächsten Gliedes definiert, würde dies bedeuten, dass grosse Gemeinschaften einen unnötig hohen Sicherheitsstandard pflegen müssen, obwohl ein Zugriff auf deren Daten durch „unsicherere“, kleinere Gemeinschaften möglich ist.	Dieser Passus ist zu löschen. Alle Gemeinschaften müssen auf dem gleichen Niveau der Sicherheit arbeiten, weil aus allen Gemeinschaften, auf alle Patientendossiers und alle darin gespeicherten Dokumente zugegriffen werden kann.
Art. 16, Seite 28	Muss die sichere Identifikation des Stellvertreters vom Identiy Provider (IdP) erfolgen? Wie stellt der Patient in diesem Fall sicher, dass es sich um den Stellvertreter handelt, den er gerne möchte? Wäre	Der Hinweis auf die zivilrechtlichen Bestimmungen ist zu konkretisieren: Stammgemeinschaften müssen im Zugangsportal für GFP die Möglichkeit anbieten, eine Vertretung nach Art. 378 ZGB zu erfassen oder zu löschen. Hierbei muss der Vertreter über ein gültiges Identifikationsmittel

	es nicht sinnvoller, die Bestimmung der Stellvertreter zumindest teilweise in die Verantwortung des Patienten zu legen?	verfügen und der Patient ein Auftrag zur Personensorge nach Art. 360 Abs. 2 und Art. 361 ZGB an den Vertreter erteilen, wobei eine elektronische Kopie des handschriftlich verfassten Auftrags ausreichend ist. Die elektronische Kopie des Auftrags ist bei der Stammgemeinschaft zu hinterlegen.
Art. 18, Seite 29	Zu Ziff. 10.2.2 TOZ: ein Export zur Archivierung mit erneutem Import der Daten durch den Patienten ist aus Sicherheits- und Datenintegritätsgründen zu verbieten. Der Patient kann mit der Vertraulichkeitsstufe „geheime Daten“ nicht mehr behandlungsrelevante Dokumente geheim stellen und diese dem Zugriff aller GFP entziehen. Will der Patient die Daten wieder zugänglich machen, so kann er die Vertraulichkeitsstufe erneut anpassen. Die Stufe geheime Daten wurde für genau diesen Zweck eingeführt.	Der Absatz beginnend mit Ziffer 10.2 der TOZ […] bis geblieben ist (vgl. Ziff. 10.2.2 der TOZ) kann ersatzlos gestrichen werden.
Art. 20 Seite 29, 30	Welchen Nachweis benötigt man, um den Patienten für tot zu erklären und das Patientendossier zu löschen? Todesschein? Wie soll die Widerrufserklärung 10 Jahre aufbewahrt werden, wenn diese formlos erfolgen kann?	Neue Formulierung: Bevor ein Dossier gelöscht wird, müssen folgende Personen schriftlich eine Aufhebungsmitteilung erhalten: Der Patient, seine Vertreter und sein Arzt des Vertrauens (Hausarzt). Bleibt die Aufhebungsmitteilung während 90 Tagen unbeantwortet, darf ein Dossier gelöscht werden. Beim Tod des Patienten muss das Todesdatum von einer Gesundheitsfachperson oder Hilfsperson erfasst werden. Im Weiteren muss eine Amtsstelle, ein Angehöriger oder ein Vertreter des Patienten der Stammgemeinschaft den Tod des Patienten bescheinigen. Will ein Patient sein Dossier aufheben, so hat er dies mit seiner Unterschrift auf einer Widerrufserklärung zu äussern. Die Unterschrift kann auch elektronisch erfolgen. Die Widerrufserklärung und die Todesbescheinigung müssen von der Stammgemeinschaft 10 Jahre aufbewahrt werden.
Art. 25, Seite 33	Muss ein Identifikationsmittel tatsächlich nach 10 Jahren neu beantragt werden? Widerspricht dem Erlasstext der	Bitte klarstellen

	besagt, dass ein Identifikationsmittel vor Ablauf „erneuert“ werden kann.	
Art. 33, Seite 26	Diese Formulierung scheint falsch. Das Identifikationsmittel kann beim Herausgeber gesperrt werden. Das Patientendossier kann für den Zugriff mit diesem Identifikationsmittel gesperrt werden. Der Herausgeber kann das Identifikationsmittel aber nicht ausschliesslich für eine Anwendung sperren und alle anderen Anwendungen weiterhin erlauben. So funktionieren diese Technologien nicht.	Die Formulierung ist missverständlich und muss korrigiert werden.

4 EDI: Verordnung des EDI über das elektronische Patientendossier EPDV-EDI

Allgemeine Bemerkungen

Die EPDV-EDI enthält viele Delegationen an das EDI. Wesentliche technische Details sind in den Dokumenten des EDI geregelt. Grundsätzlich begrüsst es die IG eHealth, detaillierte und umsetzungserprobte Spezifikationen (wie IHE dies im Prozess vorgibt) für ein System vorzugeben. Jedoch sehen wir als Industrie keine Verpflichtung des EDI, die entsprechenden Spezialisten zu rekrutieren oder weiterhin zu finanzieren. Darüber hinaus liegt kein Prozessbeschrieb vor, wie Änderungen/Anpassungen an den technischen und organisatorischen Vorgaben erfolgen sollen. Es ist der IG eHealth daher ein grosses Anliegen, dass dieser Prozess, an wen Änderungsvorschläge zu richten sind, wie diese priorisiert werden und wer den Entscheid, eine Änderung anzunehmen, fällt, zu definieren. Auch muss definiert werden, bis wann die Änderungen in den Gemeinschaften umgesetzt werden müssen. Diese Fristen sind unter Einbezug der betroffenen Kreise realistisch anzusetzen.

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art 8.	Dem Anspruch des Patienten an Einfachheit und Klarheit muss hohe Priorität eingeräumt werden, da eine umständliche Anwendung eine grosse Zugangshürde zum EPD darstellt. Daher gilt es im Rahmen der nötigen Sicherheitsanforderungen auch die Praktikabilität mittels einfachen Grundregeln/Voreinstellungen sicherzustellen. Der Anhang 8: Vorgaben für den Schutz der Identifikationsmittel muss aus dieser Perspektive dringend überarbeitet werden	Für den Erfolg des Patientendossiers ist es wichtig, sowohl sichere als auch bequeme Identifikationsmittel anzubieten. Aus der Erfahrung stellen wir fest, dass Smart Cards auf wenig Akzeptanz stossen und sich grosse betriebliche Herausforderungen in Bezug auf Kompatibilität mit einer vorhandenen IT-Infrastruktur wie auch an die Ausgabeprozesse stellen. Systeme wie mTAN oder Verfahren die biometrische oder verhaltensbasierte Mechanismen nutzen, sind de facto ausgeschlossen. Es ist sicherzustellen, dass Identifikationsmittel mit genügendem, kantonal akzeptierten Schutzniveau in Spitälern auch für den Zugriff auf das EPD verwendet werden dürfen (Rechtsgleichheit bzgl. Schutz von med. Daten kantonal wie national). Es darf nicht sein, dass hier zusätzliche Investitionen notwendig sind. Es ist zu vermeiden, wo rechtlich zulässig, dass doppelte Identifikationen (Identifikationsmittel für spitalinterne Zugriffe und separates Identifikationsmittel für EPD Zugriffe) eingesetzt werden müssen. In Zukunft sollte eine Identität, die für die eID zertifiziert ist, auch für das ePD gelten.

Bemerkungen zu den Erläuterungen		
Seite / Artikel	**Kommentar**	**Änderungsantrag**

5 EDI: EPDV-EDI Anhang 1: Kontrollzifferprüfung

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

6 EDI: EPDV-EDI Anhang 2: Technische und Organisatorische Zertifizierungsvoraussetzungen (TOZ)

Allgemeine Bemerkungen

Scope der TOZ, Systemgrenzen: Im Anhang 2: Technische und Organisatorische Zertifizierungsvoraussetzungen (TOZ) fehlt eine klare Definition der Systemgrenzen. Dies führt dazu, dass an verschiedenen Stellen im Dokument nicht klar ist, wie die entsprechenden Vorschriften auszulegen sind. Die TOZ ist hinsichtlich der Einhaltung des Scopes von EPDG und EPDV zu prüfen. Die TOZ definiert ihren Geltungsbereich nicht. Diese Definition muss vorliegen, damit alle Anbieter mit gleich langen Spiessen kämpfen und alle gezwungen sind, vergleichbar hohe Sicherheitsanforderungen zu erfüllen. Das schafft Gleichheit bei der Zertifizierung, weil der Auditor klare Richtlinien hat, nach denen er auditieren muss. Im Weiteren ist auch nicht klar, welche Kosten sich für die Teilnehmer im System ergeben für die Umsetzung und die Zertifizierung der Lösung.
Viele Vorschriften regeln gemeinschaftsinterne Angelegenheiten, die keine Relevanz zum eigentlich Zweck des EPDG haben bzw. unserer Ansicht nach nicht im Geltungsbereich des EPDG liegen.

Austritt einer Gesundheitseinrichtung: Die Idee, dass die einzelnen Dokumente der Organisation gehören, erachten wir als falsch. Sie gehören dem Patienten. Darum soll eine GFP die Dokumente nicht einfach verschieben oder löschen können. Diese Vorschrift widerspricht dem Zweck des Gesetzes: Dokumente im Patientendossier gehören den Patienten. Der Austritt einer Gesundheitseinrichtung kann nicht zu deren Löschung führen. Egal ob die Gesundheitseinrichtung einer anderen Gemeinschaft betritt oder nicht.

Identifikationsmittel (IDM): Es muss mehr Konsistenz hergestellt werden bei den Anforderungen an die Verwendung der IDM zertifizierter Herausgeber. Zudem ist es aus unserer Sicht zwingend, dass mTAN ein zugelassenes IDM ist (vgl. auch Bemerkungen zu Anhang 8). So wie die EPDV und die TOZ derzeit formuliert sind, ist mTAN ausgeschlossen. Der Anhang 8: Vorgaben für den Schutz der Identifikationsmittel muss dringend überarbeitet werden. In der vorliegenden Version sind viele Passagen so geschrieben, dass lediglich Smart Card basierte Authentisierungsmittel die Anforderungen erfüllen können. Für den Erfolg des Patientendossiers ist es wichtig, sowohl sichere als auch bequeme Authentisierungsmitttel anzubieten. Aus der Erfahrung müssen wir feststellen, dass Smart Cards auf wenig Akzeptanz stossen. Problematisch sind auch die Formulierungen in Kontext von grösseren Gesundheitseinrichtungen. Es ist unklar, ob eine Organisation, die Authentisierungsmittel für den eigenen Einsatz herausgibt, den gleichen Anforderungen unterworfen wird. Auch hier ist eine klare Definition der Systemgrenze gefordert oder nach kantonalen Gesetzen ausreichende IDM zuzulassen.

Dokumentenformate: Die Restriktionen sind sehr einschränkend. Wir würden die Definition einer für alle Gemeinschaften minimal umzusetzenden Anzahl bevorzugen anstelle einer abschliessenden Aufzählung.

Metadaten: Es fehlen die Regeln und Vorgaben für die Pflege der Metadaten (neue definieren, löschen usw.). Das Management der Metadaten ist sehr wichtig. Jede Änderung wird hohe Aufwände generieren. Die TOZ sollte Vorgaben machen, wie die Gemeinschaften diese Anpassungen der Metadaten umsetzen müssen, hinsichtlich Geschwindigkeit, Vollständigkeit etc.

Autorenrechte: Kann man grundsätzlich davon ausgehen, dass solange der Patient keine Zugriffsrechte an GFP vergibt, auch niemand etwas im EPD sieht bzw. keinen Einblick hat? Das steht so nirgends explizit geschrieben, ist aber nach Befragung der Industrie wichtig.
Die Verordnung macht keine Aussage zur Autorisierung von Autoren auf den von Ihnen publizierten Dokumenten. Darum stellt sich die Frage, ob ein Autor das Recht hat, alle von ihm publizierten Dokumente zu suchen und darauf zuzugreifen.
Folgender Use Case:

- Ein Apotheker hat das Recht erhalten den Medikationsplan eines Patienten kurz (30 Minuten) zu konsultieren. In der Nachtverarbeitung soll darum die Dispensation publiziert werden.
    - Darf die Dispensation publiziert werden, obschon der Apotheker nicht mehr autorisiert ist?
    - Wird nachträglich ein Fehler korrigiert, darf die korrigierte Version als Update publiziert werden?

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
1.1.1	Der Begriff der Gesundheitseinrichtung ist zu definieren. Insbesondere ist zu klären, ob ein niedergelassener Arzt, ein Therapeut oder eine Hebamme grundsätzlich nur als "Mitarbeiter" einer Gesundheitseinrichtung in einer Gemeinschaft teilnehmen kann.	Klarer formulieren was gemeint ist.
1.1.2.2	Diese Anforderung kann nur erfüllt werden, wenn die Dienste die entsprechenden Prozesse und technischen Mittel zur Verfügung stellen. Diese Anforderungen sind nirgends beschrieben.	Verpflichtende Anforderungen an die Dienste gemäss Art. 40 müssen in der Verordnung (oder Anhängen) formuliert werden.
1.1.3.2	Ist nicht nachvollziehbar. Tritt eine Gesundheitseinrichtung aus einer Gemeinschaft aus, dann ist es Sache der neuen Gemeinschaft, die Gesundheitseinrichtung wieder korrekt zu erfassen. Die Identifikatoren von Gesundheitseinrichtung und -fachpersonen (GLN) bleiben erhalten. Die Verknüpfung mit Dokumenten auch. Wichtig: Eine Gesundheitseinrichtung kann Ihre Dokumente nicht in eine neue Gemeinschaft mitnehmen, und zwar aus folgenden Gründen: Die Verknüpfung der Dokumente ändert sich, weil sich die ID der Affinity Domain ändert. Alle Referenzen in den Audit Logs würden verloren gehen. Damit wäre die Nachvollziehbarkeit verloren. Reine Metadaten Updates (siehe XDS.b) würden verloren gehen, weil auch die Registry gelöscht werden müsste, da die	Empfehlung: Anforderung streichen

	Einträge in der Registry auf nicht vorhandene Dokumente zeigen.	
1.1.3.2.1	Ist nicht nachvollziehbar. Tritt eine Gesundheitseinrichtung aus einer Gemeinschaft aus, dann ist es Sache der neuen Gemeinschaft, die Gesundheitseinrichtung wieder korrekt zu erfassen. Die Identifikatoren von Gesundheitseinrichtung und -fachpersonen (GLN) bleiben erhalten. Die Verknüpfung mit Dokumenten auch. Wichtig: Eine Gesundheitseinrichtung kann Ihre Dokumente nicht in eine neue Gemeinschaft mitnehmen, und zwar aus folgenden Gründen: Die Verknüpfung der Dokumente ändert sich, weil sich die ID der Affinity Domain ändert. Alle Referenzen in den Audit Logs würden verloren gehen. Damit wäre die Nachvollziehbarkeit verloren. Reine Metadaten Updates (siehe XDS.b) würden verloren gehen, weil auch die Registry gelöscht werden müsste, da die Einträge in der Registry auf nicht vorhandene Dokumente zeigen.	Empfehlung: Anforderung streichen
1.1.3.2.1	Diese Vorschrift widerspricht dem Zweck des Gesetzes: Dokumente im Patientendossier gehören den Patienten. Der Austritt einer Gesundheitseinrichtung kann nicht zu deren Löschung führen. Egal ob die Gesundheitseinrichtung einer anderen Gemeinschaft betritt oder nicht. Beispiele der "nicht elektronischen Welt": Ein Arzt gibt seine Praxis auf. Röntgenbilder und andere Dokumente, die er Patienten gegeben hat, zerfallen nicht zu Staub. Ein Kanton beschliesst ein unrentables Spital zu schliessen. Alle Dokumente die an Patienten ausgehändigt wurden entzünden sich nicht spontan.	Empfehlung: Ausscheidende Gesundheitseinrichtung muss die Daten im Repository lassen. Das Repository geht in den Besitz der Gemeinschaft über.
1.1.3.2.2	Solche Einträge dürfen gemäss Art. 9 Abs. 1 lit. c EPDV gar nicht vorkommen. Die Erläuterungen zur Verordnung deuten an, dass es technische Gründe geben könnte. Es fehlen allerdings weitere Details.	Empfehlung: diese Ausnahme ist zu löschen.
1.2.3.2	Diese Anforderung ist nicht nachvollziehbar. Beispiel: Hat ein Arzt eine SuisseID, wie soll dann ein Administrator der Gemeinschaft prüfen, ob die SuisseID funktioniert? Ist für die	Klären. Es muss etwas gefordert werden, das auch umsetzbar ist.

	Gemeinschaft relevant.	
1.2.3.3	Diese Vorschrift ist nicht nachvollziehbar. Zugriffsrechte im Patientendossier werden von Patienten verwaltet. Welche Verwaltungsprozesse sollen dabei zu einer Anpassung von Zugriffsrechten führen?	Diese Anforderung ist zu löschen.
1.2.2.5	Sind die Register MedReg etc. nicht Bestandteil des Abfrageservice HPI? Müssen die separat an den HPD angebunden werden? Wiederspruch mit dem Gesetz: Die Gemeinschaften sind für die Daten zuständig. Die Register haben eine andere Ownerschaft. Wer hat das Recht bei widersprüchlichen Daten? Wer entscheidet bei Konflikten? Hilfspersonen fehlen.	Klären, im Weiteren sind die Hilfspersonen ebenfalls in den Abfragedienst der Gesundheitseinrichtungen aufzunehmen, damit diese Gemeinschaften übergreifend identifizierbar und für den Patienten erkennbar werden.
1.3	Gemeinschaftsinterne Vorschriften fallen nicht in den Geltungsbereich des EPDG. Darum sollten dazu auch keine Vorschriften gemacht werden.	Klärung Scope der EPDV und der TOZ
1.3.1	Hilfspersonen sind auch übergreifend zu verwalten, um diese dem Patienten erkennbar zu machen.	Streichen siehe 1.2.2.5
1.4.1	Problem, dass spitalinterne Logins nicht mehr zulässig sind. Der Abschnitt regelt nur die Anforderungen der IDM für den Zugriff. Welche Anforderungen gelten für das Schreiben in ein Dossier?	Nach kantonalem Recht genügende IDM der Organisationen müssen für den Zugang zum EPD ebenfalls akzeptiert werden. Bitte IDM Anforderungen für das Schreiben von Daten beschreiben.
1.4.3.1	Diese Forderung ist im Widerspruch zu Punkt 1.4.1. In 1.4.1 gelten die Anforderungen für die IDM nach EPDG. Für 1.4.3.1 reicht ein beliebiges, starkes Authentifizierungsverfahren. Was begründet dann die hohen Anforderungen in 1.4.1 resp. die geforderten Anforderungen in Art. 22 und 23 EPDV?	Konsistenz in der TOZ herstellen oder Differenzen begründen.
1.4.3.1	Der Begriff „Bearbeitung“ sollte definiert werden. Gilt das Wissen über die Existenz von Daten als Bearbeitung? Gilt das Lesen von Daten bereits als Bearbeitung? Dies hat Implikationen an verschiedenen Stellen der TOZ.	Der Begriff „Bearbeitung“ sollte definiert werden.
1.4.3.2	Soll diese Forderung bedeuten, dass alle Gesundheitseinrichtungen, welche ein Primärsystem am Patientendossier an-	Forderung klarer formulieren.

	schliessen wollen, das entsprechende Primärsystem mit einem zertifizierten Herausgeber von Identifikationsmitteln verknüpfen müssen? Das hat immense Auswirkungen auf die Spitäler.	
2.2.1.1	Es ist unklar, was mit dem Wort „ausschliesslich“ gemeint ist, da es als doppelte Ablage interpretiert werden könnte. Dies wäre nicht zielführend, da die Kosten verdoppelt würden und das Handling in der Praxis unrealistisch und stark fehleranfällig wäre. Siehe auch 9.1.c EPDV	Dokumente des elektronischen Patientendossiers nur in ~~ausschliesslich~~ für diesen Zweck vorgesehenen Dokumentenablagen gespeichert werden;
2.2.1.2	Hier ist wohl Anhang 4 und nicht Anhang 3 gemeint.	Bitte korrigieren.
2.2.1.3	Die Einschränkung auf Ausprägung PDF/A-1 oder PDF/A-2 kann zu einer zwingenden Transformation der Daten führen. Diese Transformation birgt das Risiko eines Informationsverlustes oder Integritätsverlustes. Das System soll keine Transformation des Formats vornehmen. Als Konsequenz dürfen vom System Daten mit der Ausprägung PDF/A-1 oder PDF/A-2 akzeptiert werden. Alle anderen Ausprägungen werden abgewiesen was zu einem grossen Akzeptanzproblem bei den Benutzern führen wird.	Die Anforderung ist zu streichen.
2.3.1.1.1	Der Patient hat die Einwilligung gegeben, dass Daten im Dossier abgelegt werden. Daten können geheim publiziert werden. Diese Forderung ist zu wenig klar formuliert. Die Publikation von Dokumenten ist Sache der GFP und nicht der Gemeinschaft. Grundsätzlich sollte der Patient die GFP instruieren und nicht die Gemeinschaft. Der Begriff "bestimmte" kann von der Gemeinschaft nicht interpretiert werden. Beispiel: Darf der Patient wünschen, dass keine Dokumente welche 3 Seiten lang sind, in seinem Dossier publiziert werden?	Anforderung klarer formulieren, denn so kann sie nicht umgesetzt werden.
2.6.1.1	An dieser Stelle wird verlangt, dass ein Notfallzugriff vorgängig begründet werden muss. Aus der Sicht der IG eHealth ist diese Vorgehensweise nicht praktikabel.	Die IG eHealth fordert, dass „vorgängig“ durch „nachträglich“ ersetzt oder die Vorgehensweise vereinfacht wird (siehe Änderungsantrag zu Art. 2 EDPV).
2.6.1.2	Bedeutet dies, dass ein Arzt folgendes machen muss: • er sucht den Patienten im MPI • er deklariert einen Notfall für den Patienten • er dokumentiert den Grund des Notfalls • er bestätigt bei jedem Zugriff, dass es sich um einen Notfall handelt. Diese Forderung macht die Arbeit mit dem Patientendossier in einer Notfallstation sehr aufwendig. Es ist nicht nachvollziehbar, warum ein GFP als Spezialist jedes Mal wieder bestätigen	Antrag: Es muss für die GFP jederzeit klar sichtbar sein, dass ein Notfall deklariert ist und dass die Zugriffe mit Notfallautorisierung ausgeführt werden. Dies ist analog zu Patienten beigebrachten Dokumenten. Dort muss die GFP auch nicht jedes Mal bestätigen, dass die Quelle der Daten bekannt ist.

	muss, dass ein Zugriff gewollt ist. Benutzerfreundlichkeit beachten.	
2.8.1	Das ist sehr rudimentär und minimalistisch formuliert. Wo sind die Regeln für die Pflege der Metadaten?: neue Metadaten definieren, Metadaten löschen usw.	Antrag: Wir müssen davon ausgehen, dass Metadaten gepflegt werden. Die TOZ resp. das EDI sollte Vorgaben machen, wie die Gemeinschaften diese Anpassungen der Metadaten umsetzen müssen, hinsichtlich Geschwindigkeit, Vollständigkeit etc.
2.9.4.4	Patient Location Query [ITI-56]	Die IG eHealth fordert, den Punkt 2.9.4.4 zu streichen. Die Patient Location Query wird in Anhang 5 der EPDV-EDI explizit ausgeschlossen: 1.8.1 The Health Data Locator and Revoke Option of the Patient Location Query transaction [ITI-56] MUST NOT be used.
2.9.10	Wer kann die Rolle „Document Administrator“ wahrnehmen? Bei der Berücksichtigung von Autorenrechten wäre klar, dass jeder Autor implizit auch „Document Administrator“ der von ihm publizierten Dokumente ist. Mit dem Wegfall von Autorenrechten kann das so nicht umgesetzt werden.	Update und Delete Document sind starke Funktionen. Es muss klar sein, wer diese Funktionen ausüben darf. Bitte definieren falls nicht der Autor diese Funktion implizit erhält.
2.9.10.1	Update Document Set [ITI-57]	Gemäss Art. 1 Abs.1 EPDV muss immer eine Vertraulichkeitsstufe angegeben werden.
2.9.10.2	Delete Document Set [ITI-62]	Die IG eHealth empfiehlt den Punkt 2.9.10.2 zu streichen. Es reicht aus, die Metadaten zu ändern.
2.9.11	EPDG hat den Vertrauensraum zwischen den Gemeinschaften im Fokus. XDS.b Transaktionen sind out of scope.	Der Scope EPDG, EPDV und TOZ ist klarer zu definieren.
2.9.18.1	Record Audit Event [ITI-20]	Die IG eHealth fordert den Abschnitt „Akteure und Transaktionen der Integrationsprofile – Authentisierung von Systemen und Protokollierung von IHE-Transaktionen“ mit einem Punkt 2.9.18.2 Maintain Time [ITI-1] zu ergänzen. Dies gemäss Anhang 5 der EPDV-EDI, Punkt 1.4.2.4 ATNA Secure Application.
2.9.4.2	Diese Anforderung sollte nicht nötig sein. Punkt 2.9.1 definiert die Schnittstelle zur ZAS. Die ZAS bietet auch WebService an. Wieso nur SEDEX? Die Nutzung von SEDEX ist nicht kostenlos. Wer soll diese Kosten tragen?	Antrag: Diese Anforderung löschen.
2.9.25	Warum wird hier nicht das Profil CT (consistent time) referenziert?	CT ist eine Voraussetzung für ATNA. ATNA wird von den anderen IHE Profilen vorausgesetzt. Es würde mehr Sinn machen, dass CT die Schweizer Zeit als Quelle verwendet.
2.10.2	Gemäss Punkt 2.10.2 sind die Protokolldaten auf das erforderliche Mass zu beschränken und dürfen keine medizinischen Daten enthalten.	Für die IG eHealth stellt sich die Frage, wie das „erforderliche Mass“ an dieser Stelle definiert wird. Es gilt diesen Begriff in den Begriffsdefinitionen aufzunehmen. Andernfalls muss das erforderliche Mass in einem Betriebsreglement national geregelt werden.
2.10.3.2	Ist es korrekt, dass es genügt, wenn eine nachträgliche Ände-	Alternativformulierung: eine nachträgliche Veränderung von Protokoll-

	rung nachgewiesen werden kann?	daten muss klar erkennbar sein.
2.10.4.2	Ist es sinnvoll, dem Patienten auch abgewiesene Zugriffsversuche im Log anzuzeigen? Ist es wirklich nötig jede Suche mit den entsprechenden Suchkriterien im Log anzuzeigen, kann verwirrend sein, vor allem wenn nichts gefunden oder geliefert wurde.	Bitte präzisieren
2.10.4.2.1	Die Liste steht unter dem Fokus "Einsichtnahme durch Patient". Ist es korrekt, dass ein Patient zu wahllosen GFP anschauen kann, wann diese eingeloggt und ausgeloggt sind oder ist hier der login/logout des Patienten gemeint?	Die Formulierung des "Fokus" ist zu prüfen. Die Protokollierung ist grundsätzlich sinnvoll. statt: die Authentifizierung am System (Login/Logout) Alternative: die eigene Authentifizierung am System (Login/Logout)
2.11.1	Für die IG eHealth ist es zentral, dass Gemeinschaften sicherstellen müssen, dass die Patientenidentifikationsnummer der zentralen Ausgleichsstelle (ZAS) **nicht persistent** in den Dokumentenablagen oder Dokumentenregistern gespeichert wird. Genau so, wie dies der Erlasstext vorsieht. Die Forderung, dass die Patientenidentifikationsnummer in den Metadaten von Dokumenten persistent vorzuhalten ist, lehnt die IG eHealth entschieden ab. Folgende Gründe sprechen dagegen: • Wird die Patientenidentifikationsnummer auf allen Dokumenten vermerkt, gehen im Fall eines gewollten oder nötigen Nummerwechsels sämtliche Beziehungen verloren, d.h. Dokumente können bei einem Wechsel der Patientenidentifikationsnummer nicht mehr eindeutig einem Patienten zugeordnet werden. Aus Sicht des Datenschutzes erachtet dies die IG eHealth als problematisch. • Das Konzept, Dokumente über den MPI und lokale Schlüssel zu verbinden, ist zwar komplexer, aber erlaubt die separate Bearbeitung von Dokumenten. Dies deshalb, weil auf jedem Dokument der Name und das Geburtsdatum des Patienten vermerkt ist.	-
3.5.1.5	Der Punkt 3.5.1.5 verlangt, dass ein Zugangsportal die Möglichkeit bieten muss, strukturierte Daten sowohl im Originalfor-	Die IG eHealth erachtet „menschenlesbar“ nicht als ein Problem des Abrufs von Daten, sondern als ein Problem der Darstellung. Der Er-

	mat, als auch als menschenlesbares Format heruntergeladen werden können.	lasstext muss präzisiert werden, d.h. es muss definiert werden, was ein „menschenlesbares Format“ ist. Ist damit ein serverseitiges Rendering gemeint? Falls ja, müsste das ausformuliert werden.
3.5.2	Der Punkt 3.5.2 verlangt, dass für den Abruf von Dokumenten zur Darstellung oder zum Abspeichern zulässige Obergrenzen für die erlaubte Anzahl von Dokumenten pro Zeiteinheit („rate limits“) zu definieren sind, welche beim Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen auslösen.	Die IG eHealth ist der Ansicht, dass eine solche Obergrenze nicht zulässig ist. Weitere verfügbare Dokumente müssen erkannt und einfach abgerufen werden können.
4.10.3 ff	Gemeinschaften müssen gemäss dem Erlasstext Datenschutz- und Datensicherheitsverantwortliche bestimmen. Diese Schlüsselpersonen müssen eine Personensicherheitsprüfung (PSP) nach dem Militärgesetz durchlaufen haben. Die IG eHealth zweifelt daran, ob diese Vorgehensweise verhältnismässig ist.	Für die IG eHealth stellt sich die Frage, ob der Grundsatz der Rechtsgleichheit nicht verletzt wird, wenn auf Bundesebene ein so hohes Schutzniveau verlangt wird, gleichzeitig auf kantonaler Ebene das Schutzniveau für die Bearbeitung der gleichen medizinischen Daten jedoch viel tiefer liegt. Die IG eHealth empfiehlt diesen Punkt mit den kantonalen Anforderungen zu harmonisieren.
6.1.3.6	Gemäss Art. 20 Abs. 1 EPDV kann das elektronische Patientendossier aufgehoben werden. Bei der Aufhebung wird die Patientenidentifikationsnummer in der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) annulliert. Nach einem Widerruf zur Führung eines elektronischen Patientendossiers besteht für einen Patienten jedoch die Möglichkeit, erneut ein Dossier zu eröffnen. Bei einer Neueröffnung wird dem Patienten eine neue Patientenidentifikationsnummer zugeordnet.	Die IG eHealth begrüsst die Möglichkeit für Patienten, mehrmals ein elektronisches Patientendossier eröffnen zu können. Der Patient sollte jedoch **vor der Aufhebung** seines elektronischen Patientendossiers darauf hingewiesen werden, dass seine im Dossier abgespeicherten Daten unwiderruflich verloren gehen. Bei einer Neueröffnung muss der Patient die gewünschten Dokumente erneut in seinem elektronischen Patientendossier abspeichern.

7 EDI: EPDV-EDI Anhang 3: Metadaten

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
1.6	Auflistung der Dokumenttypen / Austauschformate	Für die IG eHealth stellt sich die Frage, ob die Liste vollständig ist. Ist sie es nicht, können nur drei Dokumententypen im elektronischen Patientendossier abgespeichert werden. Die IG eHealth fordert, dass zumindest die offiziellen Austauschformate unterstützt werden. Für einen Laborbefund im Transplantationsprozess wäre das dann z.B. urn:che:epd:2.16.756.5.30.1.1.1.1.3.4.1. Die IG eHealth fordert zudem, dass die Auflistung der Dokumententypen auch vom BAG weitergepflegt werden kann, ohne dass eine neue Verordnung notwendig wird. Die Austauschformate für den Medikationsplan oder den Austrittsbericht sind bereits geplant und müssen in den Erlasstext rasch aufgenommen werden können.
1.6	Der Begriff in Französisch „Format du document“ bezieht sich auf die Form des Dokumentes und nicht auf den Inhalt. Format XML, Word, …. Diese Bedeutung vom Format wurde insb. im Anhang 6, §3 (Indikatoren) und in der TOZ 2.2.1.3 verwendet	Antrag: Geeigneter Begriff finden. Z.B. Austauschformat Begriffe definieren und konsistent über alle Texte benutzen
1.8	Diese Liste ist als abschliessend formuliert. Das scheint wenig praktikabel. Wie soll damit umgegangen werden, wenn ein Patient ein Dokument in einer anderen Sprache hochladen will?	Die Liste kann entweder als Beispiel oder als Minimalanforderung definiert werden. Nachfolgende Liste wird im Gesundheitswesen verwendet: Referenzierung zu OID 1.0.639.1 (http://www.hl7.org/oid/index.cfm?Comp_OID=1.0.639.1)
1.9	Die Liste von Dokumentenformaten ist sehr restriktiv und es fehlen einige häufig benutze Formate.	Antrag: Die Liste von Dokumentenformaten sollte als Minimalanforderung formuliert werden.

	Beispiel: PNG, Vektorformate wie SVG Die Definition der Formate ist auch sehr unpräzis. TIFF ist unterstützt. Es wird aber nicht definiert ob und welchen Extension von TIFF unterstützt sein müssen.	

8 EDI: EPDV-EDI Anhang 5: Integrationsprofile

Allgemeine Bemerkungen

The underlying concept seems to be to expose ATNA logs to end users. This concept has been tried in Austria and it has later been changed to support a more human interpretable event log.
Since this has already been proven to be a less than ideal solution this should replaced with a two tiered approach of ATNA logs for legal purposes and some higher abstraction level of event logging for end users.

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
Anhang 5, Seite 7	Diese Vorschrift macht so keinen Sinn. Die definierten IHE Profile sind teilweise für den Einsatz innerhalb einer Affinity Domain und teilweise für den Einsatz "Cross Community" vorgesehen. Der Gesetzgeber hat festgelegt, dass das Gesetz den Bereich zwischen den Gemeinschaften regelt. Darum macht es keinen Sinn Profile zu definieren, welche ausschliesslich für den Einsatz innerhalb von Affinity Domains gemacht wurden. Zudem ist auch nicht klar, wie diese Liste von Profilen zu interpretieren ist. Muss jedes System, das in der Gemeinschaft teilnehmen will, diese Profile unterstützen? Ist es also verboten eine Lösung zu integrieren, welche HL7 Nachrichten über File Transfer übermittelt? Diese Vorschriften können von Auditoren geprüft werden und verursachen damit Kosten. Diese sollten vermieden werden.	Die Formulierung sollte unterscheiden zwischen MUSS (MUST) und SOLL (SHOULD) Profilen.

9 EDI: EPDV-EDI Anhang 5: Integrationsprofile - Nationale Anpassungen der Integrationsprofile

Allgemeine Bemerkungen

Using translated abbreviations and original abbreviations in the same text seems somewhat confusing.
Recommendation: use EPDG, EPDV, TOZ at all times (even in the IHE documentation). Maybe even add a table of abbreviations.

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
1.1.1	Die Formulierung MAY widerspricht der Dokumentations-pflicht für GFP	Aktuell: Healthcare professionals may save this data if necessary in their practice and hospital information systems outside of the electronic health records. Besser: Healthcare professionals MUST save this data if necessary in their practice and hospital information systems outside of the electronic health records.
1.1.1	must join a certified community The emphasis seems incorrect. Not only must the join a certified community. Such HP must ensure that they are certifiable themselves. Falsche Erwartungen können massiv Probleme bereiten.	Antrag: Clarify the formulation and make sure that the proper emphasis is made.
1.1.1	view their data the emphasis could be improved:	Antrag: instead of "their data" you should write "their own data".
1.1.2	Why is this called community portal index. The index lists many more informations apart from the portals. Community service index would be more appropriate since this service will provide information on all the services the community provides to third parties.	Antrag: change the terminology
1.1.2 - Figure 1	Why is this called "Unique person identification"?	clarify terminology
1.1.3	The term base community was introduced (and translated	clarify terminology

	to Stammgemeinschaft) already 3 or 4 years ago. It is unclear, why the term reference community is now used. Question: why is the term reference chosen? What does the community reference to?	
1.1.4	CCO is the only institution which is allowed to correlate the Social Security Number (AVN13) with the EPD-PID This statement is unclear. The community must provide the AHVN13 to the ZAS (EPDV Art 5.2.e). When this happens the community is able to correlate the two identifiers. Further: there are cantonal laws that allow the use of the AHVN13 for patient matching.	Antrag: delete this statement or clarify the statement so that it complies with the laws. Diese Klarstellung hat eine direkte Auswirkung auf die Umsetzung.
1.1.4	"For cross-community communication the gateways **may** correlate the MPI-ID to the EPD-PID." Why is it not **must**? Some transactions like patient discovery mandate the use of the EPD-PID as the only identifier. If this is not changed, can this lead to compatibility issues in the interfaces.	Antrag: MAY durch MUST ersetzen. wird das nicht geändert, dann kann es zu Kompatibilitätsproblemen kommen.
1.4.2.1	"Combine all Audit Trail Message entries of all Audit Trail Document entries into one single document of type ATNA Audit Trail Document Format (see chapter 1.4.4.2 on page 23)." This will not scale. The number of audit messages is strictly increasing over time.	At a minimum the sorting has to be "newest-first" and the number of returned records should be capped to a reasonable small number. Otherwise the coordinating server, which is in charge of aggregating the result, has increasingly high and non-deterministic memory requirements. Ideally the service should support server-side pagination and server-side search.
1.4.2.1	The specifications in EPDV and its appendices seem to prohibit on demand documents as very specific document formats are defined and explicit storage seems to be required.	Add the ATNA Document Type to the list of permitted types
1.4.2.1	Translate the coded information into the language preferred by the user when provide it to the user through the UI or other results like reports. What is the purpose of this requirement? The average pa-	In Austria the ATNA log is kept separate from a user compatible event log. The ATNA log is required for legal purposes. The event log is used to make events understandable.

	tient will hardly be able to interpret the contents of the ATNA audit log.	
1.4.3.2.1	Cache all audit messages... This paragraph implies several drawbacks: • Caching implies that an updated version of the document is not available for another 8 hours. If a user notices that after a log view, subsequent actions (even his own) are no longer presented, he may think that logging is flawed. • To force a particular implementation makes no sense. It is preferable to specify what the response must contain and maybe allow the option to cache this information for up to 8 hours. The implementation details should be left to the platform. The method chosen (On demand document) to implement this feature can be discussed. Alternatives would be: • XCF • Delayed Document Assembly	Improve the requirement for a more sustainable solution. Avoid to limit the freedom of the implementation and standardize the relevant aspect of the interfaces
1.4.3.2	instead of UUID this should read documentUniqueId see 3.43.4.1.2 Message Semantics in IHE TF Volume 2b	Antrag: instead of UUID this should read documentUniqueId
1.4.4.1	Why should the implementer be forced to persist an audit event in any particular format? A canonical format is only relevant for audit message exchange across communities. As long as the implementer can generate and populate the exchange format he should be free to store the data in whatever format deemed most practical.	Antrag: Remove MUST requirement to store audit event data in a predefined format.
1.4.4.1.1 Table 2	@EventDateTime – Swiss National Extension: Which time zone is used in a timestamps string representation is completely irrelevant as long as the time zone is in-	Antrag: remove the Swiss national extension.

	cluded in the string representation so downstream processes interpret it correctly. 2016-08-10T20:29:10+02:00 == 2016-08-10T18:29:10+00:00 == 2016-08-10T18:29:10Z == 2016-08-10T12:29:10-06:00 (No end-user will ever look at the string representation of the timestamp as it is persisted in the audit message. There is always a UI layer that will format dates and according to locale, preferences, etc.)	
1.5.1.1	OtherIDs From the documents of EPDV storing the EPD-PID in the MPI is a MUST requirement. Why is it a MAY requirement here?	Correct the requirement
1.7.2.1.1	This is unclear: If there are more than 5 matches zero matches a special handling like in the XCPD transaction (see IHE ITI TF-2b, chapter 3.55.4.2.2.6) is necessary.	clarify this statement
1.8.1	How will the following use case work: • A person has a health record in community A • He requires medical attention and visits a doctor that is member of a different community 1. How can the doctor find the patient in the MPI if XCPD does not support the required discovery transactions? 1. the doctor does not have the PID 2. the doctor cannot contact ZAS to obtain the PID 3. The patient may be able to supply the PID, but this is unlikely. the patient probably has a health insurance card, but this card does not contain the PID	an example for patient matching across communities should be provided

1.8.2	As the header is a suggestion by the initiating gateway to the responding gateway, i.e. the responding gateway may do whatever, why is there a hard limit of the value that can be recommended? To restrict a non-binding value seems pointless.	Remove “This values MUST NOT exceed 3 days.”
1.8.3	See 1.8.2	See 1.8.2

10 EDI: EPDV-EDI Anhang 5: Integrationsprofile - Nationale Integrationsprofile

Allgemeine Bemerkungen

Die Definition der Integrationsprofile schiesst unserer Ansicht nach klar über das Ziel hinaus. Es werden Vorschriften gemacht, wie bestimmte Dinge zu implementieren sind und es werden Dinge reguliert, die ausschliesslich Gemeinschafts-interne Problemstellungen betreffen. Die Integrationsprofile sind mit der Idee des Investitionsschutzes nicht vereinbar und verhindern tendenziell auch den Fortschritt. Innovative Lösungen werden durch die zahlreichen Vorschriften behindert.
There is a tendency to specify HOW something needs to be implemented instead of specifying expected results or interfaces.
The validity of the PPQ and ADR transactions in general is questionable as they specify communication and implementation details internal to the community.
It is unclear, if the system will be able to deal with a HP that is working for two different organizations that are members of two different reference communities. The implication is, that the same GLN appears from two different communities and that this same GLN is managed in two different branches of the HPD.

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
1	It has been specified for the Document Registries to act as Policy Enforcing Service Providers in terms of a XACML PEP. where has this been specified? how do we deal with the situation that someone, who knows all the identifiers relevant to a document can retrieve this document with the REG PEP intercepting this transaction? Example: A primary system that was authorized in the past, stored this information. It can access the document even after the authorization expired. Diese Art der Vorgaben macht es sehr schwierig, dass verschiedene Anbieter eigene Lösungen umsetzen können.	Antrag: Do not specify HOW something must be implemented. Specify the desired result instead. Example: Filtering directly on the REP yields the same result then forcing every REP access to issues a REG query.

2.2 - Signature	„an X.509 signature by a trusted entity (XUA Assertion Provider) to guaranty the confidentiality of the claims being made and unaltered content of the assertion." A digital signature does not provide confidentiality. implying wrong expectation must be avoided.	Antrag: Remove "confidentiality of the claims being made and".
2.2 - Subject	The custodian attribute has to be present in addition to the GLN/EPD-ID. Authorization decisions can only be made for GLN/EPD-IDs because those are the entities that are being authorized by patients. The custodian acts in the name of either one of those entities. In other words, the custodian has an existence dependency to a GLN or EPD-ID. this must be specified properly for cross community to work.	Antrag: Be more specific about which attributes co-exist on a subject.
2.2 – Attribute Statement	organization & organization-id: Carrying organization text and ID attributes for patients makes little sense. resource-id = EPD-PID: This assumes that there will never be any cross-patient use cases. This appears to be not very future proof. (At appears this is a concession to making bulk authorization of documents possible, which has addl. Problems. See below) Das hat direkte Auswirkungen auf die Implementierung und die Performance.	Antrag: Do not require org text and org ID attributes for patients. Drop EPD-PID as resource attribute.
2.3.2	XACML v2.0 is referenced: XACML 3.0 was published in Jan. 2013. is there a reason to use an outdated version?	we should keep up with current standards.
3.1.5	The list should include document access via the repository. Repository access is mentioned towards the end of the document, but really should be mentioned as an event that requires authorization in its own right. Das hat direkte Auswirkungen auf die Implementierung und die Performance	Antrag: Add trigger event "RetrieveDocumentSetRequest".
3.1.6.1	The approach of "bulk querying the PDP" does not scale for	The paragraph should be seen as an implementation example for small re-

	large responses, neither in terms of memory usage nor runtime. This approach requires the PEP to un-marshal the complete registry response into memory, then determine the document subsets and place requests for the subsets. The response can only be forwarded after all PDP responses are received, lest the document order seen by the client is not guaranteed to be the same as generated by the registry (not accounting for documents dropped from the response due to negative access decisions). The PEP must be able to operate on the registry response stream in order to scale. (Nothing prevents the PEP from caching the PDP decision for a given set of input parameters and to re-use it for sub-sequent access decisions of the same request. Possibly even across requests.) The bulk request approach, i.e. querying the PDP for all possible value combinations of authorization attributes also does not scale if other document attributes become part of the access decision. E.g., the document type. The number of combinations to bulk-query for grows exponentially with the number of attributes and their values. Das hat direkte Auswirkungen auf die Implementierung und die Performance	sult sets. But as the size of the result is unknown, unless fully un-marshaled into memory, it is rather useless from an implementation perspective. (Possibly the registry response has the Content-Length HTTP header set. In this case the size of the response would be known. But there is no guarantee for the header to be available. It is rather more likely that the HTTP response will have the Transfer-Encoding header set to “chunked” because the backend is also producing the response in a streaming fashion.) Another example based on response stream filtering should be added.
3.1.10	“urn:e-health-suisse:2015:error:not-holder-of-patient-policies” is to be set as the result of an “Indeterminate” PDP response. But the PDP will also return this decision value if there was an error during rule evaluation. The two cannot be distinguished based on the XACML response unless one has control over the PDP’s workings. Which one normally does not have as it is part of a XACML library. Das hat direkte Auswirkungen auf die Implementierung und die Performance	Antrag: Drop the attribute.

11 EDI: EPDV-EDI Anhang 6: Kennzahlen für die Evaluation

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

12 EDI: EPDV-EDI Anhang 7: Mindestanforderungen an die Qualifikation der Angestellten der Zertifizierungsstellen

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

13 EDI: EPDV-EDI Anhang 8: Vorgaben für den Schutz der Identifikationsmittel

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag