Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Ergebnisbericht der Anhörung

Verordnung über das elektronische Patientendossier (EPDV)

Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI)

22. März 2017

Inhaltsverzeichnis

1. Ausgangslage

Das Parlament hat das Bundesgesetz über das elektronische Patientendossier (EPDG; SR 816.1) am 19. Juni 2015 verabschiedet. Das Gesetz soll 2017 in Kraft treten. Das Eidgenössische Departement des Innern (EDI) hat am 22. März 2016 die Anhörung des Ausführungsrechts zum EPDG eröffnet. Die Anhörung dauerte bis am 29. Juni 2016. Konkret ging es um drei Verordnungen: Die Verordnung über das elektronische Patientendossier (EPDV), die Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI) und die Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV). Die EPDV regelt die Vertraulichkeitsstufen und Zugriffsrechte (1. Kapitel), die Vorgaben zu Vergabe und Verwaltung der PID (2. Kapitel), die Vorgaben an Gemeinschaften und Stammgemeinschaften (Zertifizierungsvoraussetzungen; 3. Kapitel), die Identifikationsmittel (4. Kapitel), die Akkreditierung (5. Kapitel), die Zertifizierung (6. Kapitel) sowie die Abfragedienste (7. Kapitel). Die EPDV-EDI konkretisiert die EPDV. Sie regelt ausnahmslos äusserst technische Aspekte des elektronischen Patientendossiers (EPD) und umfasst 9 Artikel mit 8 Anhängen. Die EPDFV konkretisiert die Vorgaben der Artikel 20 - 23 EPDG, welche die Finanzhilfen auf Stufe Gesetz regeln.

Dieser Bericht umfasst ausschliesslich die Anhörungsrückmeldungen zur EPDV und EPDV-EDI. Die Anhörungsergebnisse zur EPDFV sind in einem separaten Bericht zusammengefasst.

2. Anhörungsverfahren und Auswertungskonzept

In diesem Kapitel wird mittels einer tabellarischen Übersicht einerseits aufgezeigt, wie viele Stellungnahmen von welchen Teilnehmenden eingetroffen sind und andererseits die Auswertungsgrundsätze für das Kapitel 3 (Stellungnahmen zu den einzelnen Bestimmungen der EPDV und der EPDV-EDI) beschrieben.

2.1 Anhörungsverfahren

Tabelle 1: Übersicht über die eingegangenen Antworten

Kategorie	Kantone, GDK	Parteien	Gesamtschweizerische Dachverbände der Wirtschaft	Übrige Organisationen	Nicht begrüsste Organisationen und Privatpersonen	**Total**
Anzahl / Kategorie	27	3	3	30*	74**	137

*curafutura, der SVV und die **VKZS verzichteten in ihren Antworten ausdrücklich auf eine Stellungnahme

2.2 Auswertungsgrundsätze

Für ein möglichst umfassendes Gesamtbild werden die zahlreichen und inhaltlich sehr vielfältigen Stellungnahmen im vorliegenden Bericht möglichst akkurat zusammengefasst und wiedergegeben. Die im Rahmen der Vernehmlassung eingegangenen, detaillierten Stellungnahmen sind einsehbar unter:

https://www.bag.admin.ch/bag/de/home/themen/strategien-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/bundesgesetz-elektronische-patientendossier/anhoerung-ausfuehrungsrechts-bundesgesetz-elektronische-patientendossier.html

Die Stellungnahmen zu den einzelnen Artikeln der Vorlagen werden in Kapitel 3 dargestellt.

3. Stellungnahmen zu den einzelnen Bestimmungen der EPDV / EPDV-EDI

In diesem Kapitel werden die Stellungnahmen zu den einzelnen Artikeln der Vorlage präsentiert. Formulierungsvorschläge wurden wenn möglich in unverändertem Wortlaut wiedergegeben. Bei vorgeschlagenen Ergänzungen eines bestehenden Erlasstextes ist der Zusatz zum Zwecke der Transparenz unterstrichen. Generelle Änderungswünsche, Streichungsanträge und Vorschläge für zusätzliche Erlasstexte sind im Text ebenfalls erwähnt, aber nicht speziell gekennzeichnet.

3.1 EPDV

3.1.1 1. Kapitel: Vertraulichkeitsstufen und Zugriffsrechte

Die *KKA*, der *BüAeV*, die *GAeSO*, die *KAeG SG* und *HIN* erachten es als ratsam, das Kapitel 1 „Vertraulichkeitsstufen und Zugriffsrechte" mit einer zusätzlichen Bestimmung zu ergänzen. Sie schlagen einen neuen Artikel „Erfassung eigener Daten" mit folgender Formulierung vor: „Von der Patientin oder dem Patient selber erfasste Daten werden im elektronischen Patientendossier in einem separaten Ordner abgelegt. Nimmt die Patientin oder der Patient keine Zuordnung vor, so wird den von ihm eingestellten Daten die Vertraulichkeitsstufe „sensible Daten" zugewiesen und es gilt das Zugriffsrecht „erweitert". Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* plädieren zudem für die Umbenennung des Kapitels 1 in: „Vertraulichkeitsstufen und Zugang zum elektronischen Patientendossier".

Art. 1 Vertraulichkeitsstufen

[1] Die Patientin oder der Patient kann die Daten des elektronischen Patientendossiers einer der folgenden vier Vertraulichkeitsstufen zuordnen:

a. Vertraulichkeitsstufe «nützliche Daten»;

b. Vertraulichkeitsstufe «medizinische Daten»;

c. Vertraulichkeitsstufe «sensible Daten»;

d. Vertraulichkeitsstufe «geheime Daten».

[2] Nimmt die Patientin oder der Patient keine Zuordnung vor, so wird neu eingestellten Daten die Vertraulichkeitsstufe «medizinische Daten» zugewiesen.

[3] In Abweichung von Absatz 2 kann eine Gesundheitsfachperson neu eingestellten Daten die Vertraulichkeitsstufe «sensible Daten» zuweisen.

Die *SGMI* empfiehlt die Benennung eines Datenschutzverantwortlichen und schlägt vor, dass die Vorgaben des Datenschutzgesetzes gelten sollen. Eine Überregulierung sei zudem zu verhindern. Die *FMH* weist darauf hin, dass es die Ärztinnen / Ärzte sein werden, welche die Patientinnen / Patienten zur Eröffnung eines elektronischen Patientendossiers raten und diese darüber informieren resp. beraten. Diese Arbeit müsse finanziell kompensiert werden. An dieser Stelle machen die *FMH* zudem darauf aufmerksam, dass das elektronische Patientendossier zur Vereinfachung der Kommunikation zwischen Patientinnen / Patienten und Gesundheitsfachpersonen beitragen soll, anstatt Hindernisse zu errichten. eHealth und damit auch das elektronische Patientendossier soll die Patientinnen / Patienten auf ihrem medizinischen Weg begleiten, den Austausch von Informationen beschleunigen, deren Sicherheit stärken und den Zusammenhalt zwischen den Patientinnen / Patienten und der Gesundheitsfachperson verbessern. Konkret wird die Errichtung von Stellen für die Eröffnung der elektronischen Patientendossiers gefordert, welche auch die Aufklärung der Patientinnen / Patienten vornehmen.

Absatz 1: 7 Stellungnehmende[1] erachten es aus datenschutzrechtlicher Sicht als ungenügend, die Datenarten lediglich in den Erläuterungen darzulegen. Sie sprechen sich daher für die Aufnahme von Beispielen in der Verordnung aus, welche Datenarten in etwa unter welche Vertraulichkeitsstufen fallen. Zudem machen sie einen konkreten Formulierungsvorschlag für einen ergänzenden Absatz in Artikel 1. Ähnlich weisen die *SVBG*, *SWOR*, *Physioswiss* und der *SBK* darauf hin, dass die Ausführungen zu den

[1] KDSBSON, DSBAG, privatim, BE, ZG, FR, AG

Vertraulichkeitsstufen aus den Erläuterungen zum Verständnis der Einteilung sowohl für Gesundheitsfachpersonen als auch für Patientinnen / Patienten erforderlich seien. Eine kurze Erläuterung der Vertraulichkeitsstufen wünscht sich auch der Kanton *TG*. Die *FMH* weist darauf hin, dass es bei den Bezeichnungen für die Vertraulichkeitsstufen terminologische- und Übersetzungsprobleme gebe und fordert eine präzise Bezeichnung und Definition der Vertraulichkeitsstufen. Der Kanton *TI* wünscht eine genaue Definition der Datentypen. Die Beispiele im erläuternden Bericht seien nicht abschliessend und die Definition sollte in den Verordnungstext eingefügt werden. Ähnlich schreiben 6 weitere Kantone[2], dass die verschiedenen Begriffe und Beispiele einer Klarstellung bedürfen.

Die *SVBG*, *SWOR*, *Physioswiss* und der *SBK* erachten die vorgeschlagene Abstufung der 4 Vertraulichkeitsstufen als sinnvoll und *H+* sowie *senesuisse* begrüssen die Beschränkung auf die 4 Stufen. Die *K3* und der *VZK* befürchten, dass die Vertraulichkeitsstufen, Rollen und Zugriffsrechte für den Normalbürger zu kompliziert seien und empfehlen daher, die Zugriffsrechte und Vertraulichkeitsstufen zu vereinfachen. Dasselbe wünschen auch 6 Kantone[3], da die Patientinnen / Patienten ansonsten entmutigt werden könnten. 6 Stellungnehmende[4] sind der Ansicht, dass eine Unterscheidung zwischen „nützliche Daten“ und „medizinische Daten“ nicht zweckmässig sei, da es sich bei diesen beiden Begriffen nicht um Ausprägungen von Vertraulichkeit handle. International seien daher häufig nur 3 Vertraulichkeitsstufen üblich. Sie fordern dementsprechend die Anpassung auf die 3 Stufen „Normal (für alle Behandelnden einsehbar)“, „Restricted (sensible Daten; nur für Behandelnde mit erweitertem Zugriffsrecht einsehbar)“ und „Very restricted (geheime Daten; nur für die Patientin / den Patienten und allfälligen Stellvertretern einsehbar)“. Die *Tessaris* befürwortet ebenfalls eine Limitierung auf 3 Vertraulichkeitsstufen und benennt diese „open = free access“, „limited access“ und „secret = excluded access“. Für einen Verzicht auf die Unterscheidung zwischen nützlichen und medizinischen Daten spricht sich auch der Kanton *ZH* aus. Die *STSAG* schlägt ihrerseits eine Reduktion auf 3 Stufen mit den Bezeichnungen „nützlich/administrativ“, „medizinisch“ und „geheim“ vor. Der *ÄTG* und der *HÄ CH* erachten es ebenfalls als ratsam, eine Reduktion von 4 auf 3 Vertraulichkeitsstufen zu prüfen. Sie schreiben, dass grundsätzlich bereits jetzt alle medizinischen Daten als sensibel einzustufen seien, womit die Kategorien in Buchstaben b und c zusammenfallen würden. Der Kanton *TI* ist ebenfalls der Ansicht, dass medizinische Daten grundsätzlich als sensible Daten zu betrachten seien und schlägt eine Umbenennung der Stufe „medizinische Daten“ in „sensible Daten“ und der Stufe „sensible Daten“ in stigmatisierende (oder besonders sensible) Daten“ vor. 6 weitere Kantone[5] weisen darauf hin, dass Datenkategorien (administrativ, nützlich, medizinisch) und Vertraulichkeitsstufen (normal, stigmatisierend, geheim) zu unterscheiden seien. Zudem seien nach Artikel 3 Buchstabe c des Bundesgesetzes über den Datenschutz unter „données sensibles“ unter anderem auch persönliche Gesundheitsdaten aufgeführt. Die Unterscheidung zwischen sensiblen und medizinischen Daten im Verordnungsentwurf sei daher unverständlich und falsch. Es brauche eine entsprechende Anpassung. Des Weiteren gelte es zu präzisieren, um was es sich bei administrativen Daten handelt und dass diese für alle Gesundheitsfachpersonen zugänglich sind.

Die *Tessaris* schreibt, dass die „medizinischen Daten“ der Stufe „open – free access“ entsprechen und schlägt vor, lediglich die Vertraulichkeitsstufen „medizinische Daten“ (neu Buchstabe a), „sensible Daten“ (neu Buchstabe b) und „geheime Daten“ (neu Buchstabe c) zu führen. Der *VGIch* und die *SUVA* weisen darauf hin, dass die Vertraulichkeitsstufe „geheime Daten“ dem Ziel und Zweck des elektronischen Patientendossiers widerspreche und Buchstabe d folglich zu streichen sei. *Senesuisse* und *H+* beantragen, dass ca. 3 bis 5 Jahre nach der Einführung geprüft wird, ob die Stufe 4 notwendig ist. Während *senesuisse* darauf hinweist, dass diese Stufe den Zielen der eHealth-Strategie keinen Mehrwert bringe, gibt *H+* zu bedenken, dass die Wahrung der Vertraulichkeit und des Datenschutzes im Sinne der Patientinnen / Patienten höher zu gewichten sei als der freie Datenaustausch. Die *IG eHealth* und *PH CH* schreiben, dass sie die von eHealth Suisse empfohlenen 5 Vertraulichkeitsstufen unterstützt haben und mit der Streichung der Kategorie „administrative Daten“ nun die Lücke bestünde, wie ein

[2] GE, VS, VD, JU, FR, NE
[3] GE, VS, VD, JU, FR, NE
[4] HIN, BINT, Integic, HL7, IHE, LUKS
[5] GE, VS, VD, JU, FR, NE

Zugriff auf schützenswerte Informationen im MPI zu regeln sei. Die *IG eHealth* fügt zudem an, dass sie auch die 4 gewählten Stufen unterstützen könne. Es müsse allerdings geregelt werden, wie mit sensiblen Daten aus dem MPI umgegangen werde. Sie und *PH CH* schlagen einen neuen Buchstaben unter Absatz 1 zur Regelung des Umganges mit sensiblen administrativen Daten vor. Der Kanton *TI* wünscht wiederum, dass die Vertraulichkeitsstufe „administrative Daten" hinzugefügt wird, womit auch in Artikel 2 Absatz 1 das Zugriffsrecht im Zusammenhang mit diesen Daten angegeben werden müsse.

Die *IG eHealth*, *PH CH*, der Kanton *ZG* und die *Post* fordern eine abschliessende Definierung des Begriffes „Daten". Die *Post* erachtet zudem es als ratsam, die Begriffe und Definitionen in einem Glossar festzuhalten. Die Wichtigkeit klarer Begriffe unterstreicht auch der Kanton *NE*. Es gehe dabei um die Frage der Rechtssicherheit. Gemäss 7 Stellungnehmenden[6] sei sicherzustellen, dass nur bis auf Stufe Dokument Berechtigungen durchgesetzt werden. Die *IG eHealth* und *PH CH* schlagen folgende alternative Formulierung für Absatz 1 vor: „[…] die Daten, die in einem Dokument zusammengefasst sind, einer der […]". Ebenfalls für eine Ausführung des Begriffes „Daten" spricht sich die *Integic* aus und verweist auf den Anhang 3 – EPDV-EDI: Metadaten, Kapitel 1.12 „Typ des Dokumentes". Der *VGIch* wünscht die Präzisierung des Begriffes „medizinische Daten" resp. die Wahl eines weniger einschränkenden Begriffes. Der Kanton *TI* fordert, dass die Definition von Daten und Dokumente in Bezug auf die verschiedenen Vertraulichkeitsstufen direkt im Text der EPDV hinzugefügt werden.

Absatz 2: Der *KDSBSON* macht darauf aufmerksam, dass die Datenschutz- und Datensicherheitsmassnahmen grundsätzlich nicht empfohlen, sondern durch entsprechende technische Voreinstellungen vorgegeben werden sollten. Ausgehend von diesem „Privacy by Default"-Ansatz seien die Grundeinstellungen restriktiver auszugestalten. Konkret wäre in Artikel 1, Absatz 2 zu regeln, dass neu eingestellte Daten den „sensiblen Daten" zugewiesen würden und in Artikel 2, Absatz 2, dass im Falle einer fehlenden Zuweisung das Zugriffsrecht „eingeschränkt" gelte. Der *DSBAG* nennt diese Vorschläge ebenfalls und fordert deren Prüfung. Die *privatim* schreiben, dass es aus datenschutzrechtlicher Sicht unbefriedigend sei, dass ohne Aktivität der Patientinnen / Patienten quasi „alle auf alles" zugreifen können. Es müsse eine Differenzierung im Sinne von „Privacy by Default" erreicht werden. Konkret schlagen sie zwei Lösungsansätze vor, welche auch die defaultmässige Zuordnung neuer Daten in die Vertraulichkeitsstufe „sensible Daten" beinhalten. Ähnlich erachten es *Integic* und *BINT* als ratsam, neu eingestellte Daten die Vertraulichkeitsstufe „Restricted" zuzuweisen, falls die Patientin / der Patient keine Zuordnung vornimmt. Zudem könne die Patientin / der Patient die Option wählen, dass die Gesundheitsfachperson die Vertraulichkeitsstufe festzulegen hat. Falls diese keine Zuordnung vornimmt, soll ebenfalls die Stufe „Restricted" gelten. Der Kanton *TG* schreibt, dass als Standardeinstellung entweder die Vertraulichkeitsstufe „sensible Daten" oder „geheime Daten" gewählt werden sollte. Die *FMH* verweist generell darauf, dass eine Standardeinstellung gewählt werden sollte, welche sich stärker an den Bedürfnissen der Mehrheit der Patientinnen / Patienten orientiere. Die *Tessaris* schlägt vor, dass Daten, die neu in das elektronische Patientendossier eingestellt werden und bei denen keine Zuordnung in eine Vertraulichkeitsstufe vorgenommen wurde, der Stufe „sensible Daten" zugewiesen werden.

Gemäss dem Kanton *BS* stellt sich aufgrund der „Privacy by Default"-Thematik die Frage, ob auf eine Default-Einstellung der Vertraulichkeitsstufe bei der Einstellung von Daten gänzlich zu verzichten sei. Mit einer differenzierten Vergabe der Vertraulichkeitsstufe durch die Gesundheitsfachperson und Gesundheitseinrichtung sowie einem Verzicht auf eine generelle Einstufung als „sensible Daten" könne verhindert werden, dass viele „normal" zugriffsberechtigte Gesundheitsfachpersonen auf die elektronischen Patientendossiers zugreifen, ohne darin Daten vorzufinden, was zu verhindern sei. Der Kanton *FR* weist darauf hin, dass der „Privacy by Default"-Ansatz mit den Zielen des elektronischen Patientendossiers im Konflikt stehe und deshalb eine Interessensabwägung nötig sei. 10 Stellungnehmende[7] lehnen den „Privacy by Default"-Grundsatz als nicht zielführend ab. Der Kanton *SO* fügt an, dass davon ausgegangen werde, dass die in Artikel 3 EPDG vorgesehene, angemessene Information auch die standardmässige Vertraulichkeitsstufe (sowie die standardmässigen Zugriffsrechte gemäss Art. 2 Abs. 2 EPDV) umfasse. Der Kanton *AR* schreibt wiederum, dass „Privacy by Default" nicht abgelehnt werde.

6 IG eHealth, PH CH, K3, VZK, ZG, Post, SMCF

7 GDK, BL, GL, LU, OW, UR, SZ, NW, SO, SH

Gemäss 10 Stellungnehmenden[8] müsse davon ausgegangen werden, dass ein Grossteil der Patientinnen / Patienten die Vertraulichkeitsstufen nicht selbst verwalten möchte und daher auch die Möglichkeit bestehen sollte, dass Gesundheitsfachpersonen Daten der Stufe „nützliche Daten" zuweisen können. 9 Stellungnehmende[9] erachten es zudem als prüfenswert, ob die standardmässige Zuordnung der Vertraulichkeitsstufe auch pro Dokument unterschiedlich vorgenommen werden könnte, dies beim Upload automatisiert auf Basis dessen Metadaten. Der *HÄ CH* und die *ÄTG* erachten die in Absatz 2 der Erläuterungen festgehaltene Möglichkeit, neu eingestellten Daten per Default die Vertraulichkeitsstufe „sensible Daten" zuzuweisen, als heikel. Es könnten dadurch den Gesundheitsfachpersonen evtl. ungewollt ein Grossteil von medizinischen Informationen vorenthalten werden, womit lediglich die manuelle, einzelne Zuweisung dieser Stufe möglich sein sollte. *Santésuisse* gibt zu bedenken, dass die Regelung, wonach sich von der Patientin / dem Patienten jeder Dokumenttyp jeder Vertraulichkeitsstufe zuordnen lässt, zu Unübersichtlichkeit führen könne. Die Zuordnung von wichtigen Informationen in eine Vertraulichkeitsstufe ohne Zugriffsrecht könnte zu kritischen medizinischen Situationen führen. Ein für alle berechtigten Gesundheitsfachpersonen ersichtlicher Hinweis auf allenfalls zusätzlich vorhandene Informationen könne solche Situationen möglicherweise verhindern. Der Kanton *FR* schlägt zudem die Aufnahme eines zusätzlichen Absatzes vor, um die Information und das Verständnis der Patientinnen / Patienten sicherzustellen, was die Vertraulichkeitsstufen für eine Bedeutung haben.

Die *Post* und die *IG eHealth* befürchten, dass der in Absatz 2 beschriebene Mechanismus so nicht umsetzbar sei. Jedes Dokument müsse zuerst geprüft werden, bevor eine Vertraulichkeitsstufe zugeordnet werden könne. Die *Post* fügt an, dass die Gesundheitsfachpersonen neu publizierte Dokumente innert Sekunden lokal speichern können und die Patientin / der Patient dies im manuellen Prozess nicht verhindern könne. Das Ziel müsse daher sein, dass Gesundheitsfachpersonen bereits vorab wissen, welche Vertraulichkeit die Dokumente haben sollen. Die *Post* und die *IG eHealth* machen folgenden, konkreten Formulierungsvorschlag für Absatz 2: „Ohne andere Anweisungen der Patientin oder des Patienten, publizieren Gesundheitsfachpersonen Dokumente mit der Vertraulichkeitsstufe „medizinische Daten"". Eine alternative Formulierung schlägt *PH CH* vor: „Neu eingestellte Daten werden, sofern die Gesundheitsfachperson nicht anderes zuweist, mit der Vertraulichkeitsstufe „medizinische Daten" gespeichert."

Der *VAKA* beantragt, dass Patientinnen / Patienten eine Einstellung wählen können, mittels derer sie allen registrierten Gesundheitsfachpersonen die Zugriffsstufe „normal" erteilen und sämtliche neuen Dokumente standardmässig in die Vertraulichkeitsstufe „medizinische Daten" zuweisen können. Es sei zu betonen, dass Personen, welche die Zugriffsrechte detailliert verwalten möchten, dies weiterhin tun können. Als mögliche Sicherheitsmassnahmen wäre gemäss dem *VAKA* denkbar, dass die Patientinnen / Patienten periodisch eine Liste erhalten mit einer Übersicht, wer auf ihre elektronischen Patientendossiers zugegriffen hatte. Die *Tessaris* plädiert dafür, dass die Patientin / der Patient beim Abschluss einer Behandlung Art und Umfang der Aufnahme der neuen Daten im elektronischen Patientendossier festlegen können sollte. Die Einwilligung der Aufnahme der Behandlungsdaten ins elektronische Patientendossier sei zudem schriftlich festzuhalten und von den Patientinnen / Patienten zu unterzeichnen. Die aufgenommenen Daten seien nach dem Stand der Technik stark zu verschlüsseln. Darüber hinaus soll die Aufnahme von Daten aus vergangenen Behandlungen ins elektronische Patientendossier verlangt werden können. Der Kanton *ZH* gibt zu bedenken, dass nicht geregelt sei, was bei Urteilsunfähigkeit geschieht. Regelungen über den Umgang mit Urteilsunfähigkeit seien in das Ausführungsrecht aufzunehmen resp. mindestens Überlegungen dazu in den Erläuterungen zu ergänzen. Ebenfalls seien Regelungen über den Umgang mit elektronischen Patientendossiers von Jugendlichen / jungen Erwachsenen, insbesondere der Zeitpunkt und die Art und Weise der Übergabe der Kontrolle von den Eltern auf diese, relevant.

Absatz 3: Die *Integic*, die *HL7* und *IHE* bemängeln, dass hier ein Entscheid der Patientin / des Patienten übersteuert werde. Sie, *Bleuer* sowie die *Tessaris* fordern die Streichung von Absatz 3. Die *Integic* fordert, sofern Absatz 3 nicht gestrichen wird, einen Zusatz, dass die Patientin / der Patient über neue

[8] GDK, BL, GL, LU, OW, UR, SZ, NW, ZG, SH
[9] GDK, BL, GL, LU, OW, UR, SZ, NW, SH

„Very restricted"-Daten zu benachrichtigen sei. Die *SPO* und die *FRC* machen geltend, dass das Einverständnis der Patientinnen / Patienten wichtig sei. Die *SPO* macht folgenden Formulierungsvorschlag: „[…] kann eine Gesundheitsfachperson im Einverständnis der Patientin oder des Patienten neu eingestellte […]" und die *FRC* folgenden: „[…] le dossier électronique du patient peut, avec l'accord du patient, leur attribuer le niveau de confidentialité „données sensibles". Ähnlich empfiehlt *pharmaSuisse* folgende Formulierung: „[…] eine Gesundheitsfachperson im Auftrag einer Patientin oder eines Patienten neu eingestellte […]". Dies könne bspw. im Rahmen der Einwilligung zur Führung eines elektronischen Patientendossiers gemäss Artikel 15 erfolgen. Die *K3* und der *VZK* machen darauf aufmerksam, dass es im Spitalumfeld nicht möglich sein werde, dass einzelne Gesundheitsfachpersonen die Daten bzw. Dokumente einstellen und fordern daher folgenden Zusatz in Absatz 2: „[…] eine Gesundheitsfachperson oder eine Gruppe von Gesundheitsfachpersonen neu eingestellte Daten […]". Die *PKS* schreibt, dass ein Spital in der Lage sein müsse, die Zuordnung von Vertraulichkeitsstufen zu Dokumenten automatisch durch eine Applikation und durch verschiedene Gesundheitsfachpersonen sowie deren Hilfspersonen vornehmen zu lassen. Sie und die *SVP* fordern die Streichung der Einschränkung auf die Zuordnung zur Stufe „sensible Daten". Die *Tessaris* schlägt einen neuen Artikel vor: „Die Patientin oder der Patient kann die Vertraulichkeitsstufe für Daten im elektronischen Patientendossier jederzeit ändern. Die Änderung wird der für die betreffende Behandlung zuständigen Gesundheitsfachpersonen automatisch angezeigt."

Mit Blick auf Artikel 2 schreiben *H+* und *senesuisse*, dass sie den Ansatz, dass für die Grundeinstellung ohne spezifischen Patientenwunsch das Zugriffsrecht „normal" gesetzt wird, begrüssen. Eine Erweiterung auf zusätzliche Stufen sei zu Gunsten einer einfachen Handhabung zu verwerfen. *HIN* äussert sich ebenfalls bereits an dieser Stelle zu Artikel 2. Sie schlagen folgenden ergänzenden Punkt vor: „Nimmt die Patientin oder der Patient keine weitere Einschränkung vor, kann die Gesundheitsfachperson die ihr zugewiesenen Zugriffsrechte an Hilfspersonen delegieren, sofern deren Zugehörigkeit zur Gesundheitsfachperson gemeinschaftsintern verwaltet wird". Als Ergänzung zu Artikel 3 wünschen sie folgende Ergänzung: „Die Patientin oder der Patient kann: einzelnen Gesundheitsfachpersonen untersagen, die Zugriffsrechte an Hilfspersonen zu delegieren".

Art. 2 Zugriffsrechte

[1] Die Patientin oder der Patient kann Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen folgende Zugriffsrechte zuweisen:

a. «eingeschränkt»: Zugriff auf die Vertraulichkeitsstufe «nützliche Daten»;

b. «normal»: Zugriff auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten»;

c. «erweitert»: Zugriff auf die Vertraulichkeitsstufen «nützliche Daten», «medizinische Daten» und «sensible Daten».

[2] Nimmt die Patientin oder der Patient keine Zuweisung vor, so gilt das Zugriffsrecht «normal».

[3] Die Zugriffsrechte gelten bis zum Entzug durch die Patientin oder den Patienten.

[4] Tritt eine Gesundheitsfachperson einer Gruppe von Gesundheitsfachpersonen bei, so erhält sie das mit dieser Gruppe verbundene Zugriffsrecht. Verlässt eine Gesundheitsfachperson eine Gruppe, so wird ihr das mit der Gruppe verbundene Zugriffsrecht entzogen.

[5] In medizinischen Notfallsituationen können Gesundheitsfachpersonen auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten» zugreifen. Sie müssen einen solchen Zugriff vorgängig begründen.

HIN und *santésuisse* wiederholen die bereits beschriebenen Bemerkungen zu Artikel 1 und die *FMH* ihre einleitend zu Artikel 1 aufgeführte Stellungnahme. *PH CH* und die *IG eHealth* wünschen einen Absatz 6 mit folgendem Inhalt: „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". Die *KKA*, der *BüAeV* und die *GAeSO* schlagen folgenden zusätzlichen Absatz für Artikel 2 vor: „Nimmt die Patientin oder der Patient keine weitere Einschränkung vor, kann die Gesundheitsfachperson die ihr zugewiesenen Zugriffsrechte an Hilfspersonen delegieren, sofern deren Zugehörigkeit zur Gesundheitsfachperson gemeinschaftsintern verwaltet wird". Die *SPO* fordert folgende zusätzlichen Absätze: Absatz

6: „Der Patientin und dem Patienten ist jederzeit Einblick auf das Zugriffsprotokoll gemäss Artikel 8 Absatz 1 EPDG zu ermöglichen“. Absatz 7: „Im Streitfall muss der Nachweis für den rechtmässigen Zugriff von der Gesundheitsfachperson erbracht werden“. *Physioswiss* begrüsst explizit die Absätze 1 bis 4. Der Kanton *TI* gibt zu bedenken, dass eine Gesundheitsfachperson ohne Zugriffsrecht auf das elektronische Patientendossier, welche ein einzelnes Dokument erstellt hat, bei einem Fehler das Dokument später noch ändern können sollte. Die *SGMI* gibt zu bedenken, dass bei dieser Regelung die Patientin / der Patient die Verantwortung für nicht zur Verfügung gestellte Informationen, welche unter Umständen die Behandlungssicherheit gefährden könnten, trage. Ähnlich fordert die *STSAG* die Benennung der Verantwortlichkeit, wenn Patientinnen / Patienten Daten als geheim klassifizieren, in einem zusätzlichen Absatz. Zudem sprechen sie sich dafür aus, dass im Notfall auch auf die geheimen Informationen zugegriffen werden darf.

14 Stellungnehmende[10] weisen darauf hin, dass Regelungen betreffend urteilsunfähigen Personen und Kindern fehlen und fordern die Aufnahme dieser Thematik. Gemäss 9[11] dieser Stellungnehmenden beschäftige sich das Ausführungsrecht bislang nämlich nicht mit der Frage, ob und unter welchen Voraussetzungen die Rechte auf Verwaltung des Dossiers auch ohne Einwilligung resp. gegen den Willen einer Patientin / eines Patienten durch einen Stellvertreter nach Artikel 3 Buchstabe g ausgeübt werden könne. Die *K3*, der *VZK*, der Kanton *ZG* und der *ZAD* wünschen zudem, dass in der Verordnung auch der Umgang mit verstorbenen Personen geregelt wird. Für *K3* und den *VZK* stellt sich zusätzlich die Frage, ob es ein Dossier für Menschen ohne Papiere geben werde.

Absatz 1: Die *Insel* bemängelt, dass die Einrichtung von drei Zugriffsrechtsstufen unnötig kompliziert scheine. Es sei davon auszugehen, dass die Patientin / der Patient sensible Daten, die er von der Einsichtnahme durch Drittpersonen ausschliessen möchte, gar nicht erst aufschaltet. Zudem sei zu bedenken, dass die Gesundheitseinrichtungen wenig oder gar nicht Gebrauch von einem elektronischen Patientendossier machen werden, wenn dieses lückenhaft ist. Sie würden sich auf ihre Primärsysteme stützen. Sie fordern die Streichung von Buchstaben a in Absatz 1. Der *HÄ CH* und die *ÄTG* weisen darauf hin, dass aufgrund ihres Vorschlages aus Artikel 1 Absatz 1, die Buchstaben b und c zusammenzulegen, bei Artikel 2 Absatz 1 lediglich 2 Wahlmöglichkeiten bestünden. Sie geben zu bedenken, dass die Zuordnung von Zugriffsrechten in der angedachten Form ein komplexer und anspruchsvoller Vorgang sei, welcher die Patientinnen / Patienten überfordern dürfte. Sie fordern dementsprechend eine Vereinfachung. *PharmaSuisse* und der Kanton *ZH* empfehlen, dass ein Leistungserbringer darüber informiert werden müsse, wenn dieser auf gewisse Daten nur einen eingeschränkten Zugriff hat. Dabei sei ihm insbesondere auch mitzuteilen, auf was für Inhalte er keinen Zugriff hat. Zusätzlich müsse es gemäss *pharmaSuisse* durch Logfiles möglich sein nachzuvollziehen, welche Informationen einem Leistungserbringer zu einem bestimmten Zeitpunkt zur Verfügung gestanden sind. Die *Integic* fordert eine Anpassung auf die 3 international üblichen Vertraulichkeitsstufen (EPSOS). Die Buchstaben a bis c von Absatz 1 seien demnach wie folgt umzuformulieren: „a. „eingeschränkt“: Zugriff auf die Vertraulichkeitsstufe „Normal“; b. „normal“: Zugriff auf die Vertraulichkeitsstufen „Normal“ und „Restricted“; c. „erweitert“: Zugriff auf die Vertraulichkeitsstufen „Normal“, „Restricted“ und „Very restricted“. *PH CH* macht geltend, dass die Einführung von Begriffen für die Zugriffsrechte keinen Sinn mache und fordern folgenden, alternativen Text für Absatz 1: „[…] von Gesundheitsfachpersonen wahlweise den Zugriff auf nur nützliche Daten, nützliche und medizinische Daten oder auf nützliche, medizinische und sensible Daten gewähren“. Die Buchstaben a bis c wären ebenso wie der Absatz 3, welcher neu in den Absatz 2 integriert werden könne, zu streichen. Die *Tessaris* schlägt vor, dass alle mit der Behandlung der betreffenden Patientin / Patienten befassten Gesundheitsfachpersonen auf „medizinische Daten“ zugreifen können sollten, vorausgesetzt, dass die Patientin / der Patient dies nicht vorgängig für alle oder eine bestimmte Gesundheitsfachperson untersagt hat. Zudem solle die behandelnde Gesundheitsfachperson auch auf „sensible -“ oder „geheime Daten“ zugreifen können, wenn die Patientin / der Patient dem Zugriff vorgängig zugestimmt hat. Die *KAeG SG* weist darauf hin, dass gewisse Einträge nicht mehr sachgerecht erfolgen könnten, falls die Patientin / der Patient darauf zugreifen kann. Zudem wirft sie die Frage auf, wie bei einem Verlust der Karte auf die Daten zugegriffen werden könne und ob die

[10] BL, GDK, GL, OW, UR, VAKA, NW, FR, BE, K3, VZK, ZG, ZAD, TG
[11] BL, GDK, GL, OW, UR, VAKA, NW, BE, TG

Speicherung in einer Cloud-Lösung erfolge.

11 Stellungnehmende[12] betrachten das Konstrukt „Gruppen von Gesundheitsfachpersonen" als kompliziert und aufwändig. 9 dieser Stellungnehmenden[13] wünschen die Prüfung einer Vereinfachung, während der Kanton *ZH* und der *ZAD* die ersatzlose Streichung dieses Konstruktes fordern. Der Kanton *ZH* macht folgenden alternativen Formulierungsvorschlag für Absatz 1: „Die Patientin oder der Patient kann Leistungserbringern und Gesundheitsfachpersonen folgende Zugriffsrechte zuweisen: […]". Gemäss dem Kanton *TI* sei es notwendig, den Ausdruck „Gruppe von Gesundheitsfachpersonen" zu definieren und den Patientinnen / Patienten die Nutzung dieser Funktion verständlich zu machen. Eine Präzisierung des Begriffes „Gruppe" fordern auch 6 weitere Kantone[14]. Gemäss diesen stelle die Tatsache, dass die Zugriffsrechte nicht an ganze Institutionen erteilt werden können, insbesondere Spitäler vor Machbarkeitsprobleme. Sie wünschen folgenden Zusatz für Absatz 1: „Le patient peut accorder à des institutions, des professionnels […]" und Absatz 4 soll neu folgendermassen lauten: „[…] un groupe ou une institution reçoit les droits d'accès accordés à ce groupe ou à l'institution."

Die Absätze 1 und 4 seien dahingehend zu ergänzen, dass die Bestimmungen sowohl für Gruppen als auch für Gesundheitseinrichtungen gelten. Die *SMCF* ist der Ansicht, dass aus praktischen Gründen keine individuellen Zugriffsrechte innerhalb einer bestimmten Gruppen bestehen sollten. Der Kanton *AG* bezeichnet die Gruppenzugriffsrechte als sehr wichtig für die Praxis. Das Abfragen der Gruppenzusammensetzung erscheine datenschutzrechtlich korrekt, könne jedoch zu einem Mehraufwand für die Gemeinschaft führen. Die *PKS* sind der Ansicht, dass die Regelungen der Zugriffsrechte weder für die Behandlungsbedürfnisse von Patientinnen / Patienten, noch für die Prozesse im Spital angemessen und praktikabel seien. Sie schlagen vor, dass die Grundeinstellungen den vollen Zugriff auf alle medizinischen Daten ermöglichen sollen und die Patientinnen / Patienten dies bei Bedarf einschränken können. Die momentane Einschränkung auch auf sensible Daten sowie die Begründungspflicht erschwere die Informationsbeschaffung im Notfall unnötig.

Absatz 2: Der *KDSBSON*, der *DSBAG*, die *privatim* sowie der Kanton *FR* wiederholen an dieser Stelle ihre Kommentare von Artikel 1 Absatz 2 bezüglich der „Privacy by Default"-Thematik.

Für den *SVBG*, *Physioswiss*, *SWOR*, den *SBK* sowie *H+* sei es begrüssenswert, die Zugriffsrechte mit der Standardeinstellung „normal" festzulegen. Die *Post* beantragt wiederum, dass ohne Zuweisung das Zugriffsrecht „eingeschränkt" gilt. Die *Tessaris* schreibt, dass dieser Absatz ersatzlos gestrichen werden könne, da sich der eingeschränkte Zugriff auf Daten der Vertraulichkeitsstufe „sensible Daten" aus ihrem Redaktionsvorschlag zu Artikel 1 Absatz 2 ergebe. Die *FMH* wiederholt an dieser Stelle ihren Kommentar zu Artikel 1 Absatz 2.

Absatz 3: Der *KDSBSON*, der *DSBAG*, die *privatim* sowie der Kanton *ZG* weisen darauf hin, dass die Einräumung von Zugriffsrechten nicht unbefristet erfolgen sollte. Zudem sei eine Informationsmeldung an den Patienten / die Patientin vor Fristablauf der Zugriffsrechte zu prüfen. Sie schlagen folgende Anpassung von Artikel 3 Buchstabe a vor: „Die Zugriffsrechte werden den einzelnen Gesundheitsfachpersonen für längstens zwei Jahre eingeräumt". Für eine Begrenzung der Maximaldauer der jeweiligen Zugriffsrechte spricht sich auch der Kanton *TG* aus. Die *Tessaris* wünscht die Streichung des Absatzes, da sich die Änderung der Vertraulichkeitsstufen und damit der Zugriffsrechte oder deren Aufhebung aus ihrem vorgeschlagenen Artikel 1 Absatz 3 ergebe. Der Absatz 3 von Artikel 2 könne neu folgendermassen lauten: „Die Patientin oder der Patient kann eine namentlich bezeichnete Gesundheitsfachperson oder eine Gruppe von Gesundheitsfachpersonen zeitweilig oder dauernd vom Zugriff auf ihr oder sein elektronisches Patientendossier ausschliessen".

Absatz 4: Die *privatim*, der *KDSBSON* und der *DSBAG* weisen darauf hin, dass im Falle der Beibehaltung von Gruppenberechtigungen, auch zwingend die Möglichkeit eines „Opt-out" gemäss Artikel 3

[12] BL, GL, LU, OW, UR, ZG, SZ, NW, GDK, ZH, ZAD
[13] BL, GL, LU, OW, UR, ZG, SZ, NW, GDK
[14] GE, VS, VD, JU, FR, NE

Buchstabe f bestehen bleiben müsse. Der Kanton *TG* ist der Meinung, dass die automatische Gruppenzuteilung und die entsprechende Rechteübernahme betreffend dem Berufsgeheimnis problematisch sein könnten und macht ein Beispiel dazu. Es wird eine Lösung gefordert, welche das Berufsgeheimnis in jedem Fall garantiere.

Der *KSSG* weist darauf hin, dass die Präsentation der Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen bei einer grossen Organisation nicht überschaubar sei. Personalwechsel seien zudem derart häufig, dass die Patientinnen / Patienten zu viele Informationen erhalten würden und überfordert wären. Deshalb sei Artikel 8 mit einem zusätzlichen Buchstaben zu ergänzen, welcher besagt, dass das BAG Gemeinschaften aus Gründen der Übersichtlichkeit auf Antrag erlauben könne, den Patientinnen / den Patienten nur einen Teil der Gesundheitsfachpersonen zu publizieren. Zudem stelle sich betreffend der Informationspflicht gemäss Artikel 8 Buchstabe f für Artikel 2 Absatz 4 die Frage, ob Rechte sofort erteilt werden, oder nicht. Der *KSSG* schlägt folgende Ergänzung von Absatz 4 vor: „[…] verbundene Zugriffsrecht, ohne besondere Bestätigung durch die Patientin oder den Patienten. Verlässt eine […]". Der *VGIch* weist darauf hin, dass eine Gesundheitsfachperson bei automatischem Gruppenzugriffsrecht Zeit habe, Informationen einer Patientin / eines Patienten in das Primärsystem zu übertragen, bis diese / dieser die Möglichkeit habe, die Gesundheitsfachperson auszuschliessen. Er schlägt die Schaffung echter Gruppen vor, welche kollektiv sind. Die Patientin / der Patient müsse sich entscheiden, ob sie / er sich darauf einlässt, oder nicht. Die *ISSS* schlägt vor, dass ein neuer Absatz formuliert wird, welcher besagt, dass die Gemeinschaften den Patientinnen / Patienten auf Verlangen eine Personalliste vorlegen müssen, damit diese über die Zuweisung von Zugriffsrechten von Gesundheitsfachpersonen oder Gruppen entscheiden können. *PH CH* und die *IG eHealth* bemängeln, dass die Patientinnen / Patienten in den Grundeinstellungen über alle Gruppenänderungen, aber nicht über Notfallzugriffe informiert werden. Das führe zu einer Informationsflut gegenüber den Patientinnen / Patienten und einer persönlichkeitsverletzenden Transparenz der Versetzung von Gesundheitsfachpersonen. Sie schlagen vor, Absatz 4 unverändert zu lassen, in Artikel 3 jedoch die Optionen anzupassen. *Lovis* ist der Meinung, dass keine „Black List" für den Ausschluss von einzelnen Personen einer Gruppe bestehen sollte.
Die *K3* und der *VZK* weisen darauf hin, dass nicht ersichtlich sei, ob die Gesundheitsfachpersonen gleichzeitig mehreren Gruppen angehören können und wünschen, dass dies (mit einem Identifikationsmittel) möglich sein solle. Zudem sei für Spitäler wichtig, dass der Zugriff auf die elektronischen Patientendossiers für das ganze Spital, eine Gruppe innerhalb des Spitals oder für einzelne Gesundheitsfachpersonen erteilt werden könne und im Normalfall der Zugriff standardmässig für das ganze Spital gewährt werden solle. An dieser Stelle weisen die beiden Stellungnehmenden zudem darauf hin, dass die Zugriffsrechte auch für Hilfspersonen gelten müssen. Dies sei in der Verordnung zu ergänzen, da es bis jetzt nur im Anhang 2 (TOZ) Ziffer 1.3 der EPDV-EDI erwähnt sei. Ebenfalls müsse sichergestellt werden, dass Personalabteilungen von Spitälern auf eine einfache Art und Weise Identitätsprüfungen (Art. 23 EPDV) vornehmen können sowie geeignete Identifikationsmittel (Art. 22 EPDV) abgeben oder erneuern (Art. 25 EPDV) können.

Absatz 5: Das *BRH* bezeichnet den Zugriff in Notfallsituationen als umständlich resp. unklar und wünscht eine konkretere Beschreibung der Sicherungselemente. Zudem seien die zeitlichen Aufwände in der Notfallsituation bei Durchlauf solcher Sicherheitsbarrieren anzugeben. Der *VAKA*[15] spricht sich dafür aus, dass im Notfall standardmässig auch die sensiblen Daten zur Verfügung stehen sollten. S*enesuisse* macht geltend, dass der Wortlaut zu wenig klar erscheine, um damit die Rechte betroffener Gesundheitsfachpersonen zu regeln. Während in Absatz 5 nur auf „nützliche" und „medizinische" Daten zugegriffen werden dürfe, stehe gemäss Artikel 3 Buchstabe b die Regelung des Zugriffsrechts auch für Notfälle vollständig in Patientenhand. Besser wäre eine auf medizinische Notfälle angepasste Regelung für medizinische Notfälle. Der Kanton *ZG* fordert in den Erläuterungen die Klarstellung, dass bei Zugriffen in medizinischen Notfallsituationen Artikel 24 EPDG nur zur Anwendung kommt wenn offensichtlich ist, dass es sich nicht um eine Notfallsituation handelte.

[15] Ohne Bethesda

Der *VAKA* schreibt, dass es für einen Zugriff im Notfall eine nochmalige Anmeldung bedürfe. Eine weitere Begründung scheine obsolet, womit der Satz: „Sie müssen einen solchen Zugriff vorgängig begründen“ aus dem Absatz zu streichen sei. Ebenfalls der Meinung, dass eine Begründung für einen Zugriff im Notfall weggelassen werden könne, sind die *K3*, der *VZK*, der Kanton *ZH* sowie der *ZAD*. Die *ASPS*, der *Spitex* und die *BINT* weisen darauf hin, dass die Hürden einer Begründung tief sein müssen, damit der Zugriff rasch erfolgen könne. Strukturierte Vorgaben für die Begründungen seien zudem einfacher handhab- und auswertbar. Wie auch die *BINT* schlagen sie eine einfache Begründung im Notfall vor, oder alternativ die Möglichkeit einer nachträglichen Begründung. Ähnlich schreiben die *FMH* und *Physioswiss*, dass sie eine vorgängige Begründung eines Notfallzugriffs als nicht zweckmässig betrachten. Die systematische, nachträgliche Information und allfällige Begründung bei Verdacht auf missbräuchlichen Zugriff müsse als Lösung genügen. 6 Kantone[16] fordern ausserdem, dass der Teil vorgängig resp. „au préalable“ aus Absatz 5 gestrichen wird. Der Kanton *ZG* wünscht die Klarstellung, dass an den Inhalt und den Umfang der Begründung keine hohen Anforderungen gestellt werden. Es bestehe sonst das Risiko, dass Gesundheitsfachpersonen im Zweifelsfall nicht auf das elektronische Patientendossier zugreifen werden. Die *HL7*, *IHE* und die *Integic* wünschen betreffend der Begründung bei einem Notfallzugriff eine Vorgabe zur Form und Ausführlichkeit der Dokumentation, um eine sträfliche Verwendung einzugrenzen. Zudem sind sie wie auch die *SGMI* der Ansicht, dass als Alternative für eine vorgängige Begründung eine kurze Bestätigung des Notfalles (1 Klick) denkbar wäre und eine ausführliche Rechtfertigung erst im Nachhinein erfolgen solle. Die *Post* hält eine Begründung für sinnlos und schlägt dafür eine automatische Information an den Arzt des Vertrauens und an die Patientinnen / Patienten vor. Im Notfall müsse der Wille, dass ein Notfallzugriff mit Notifikation gemacht wird, bestätigt werden (Haken setzen und „OK“ drücken). Der Kanton *AG* weist darauf hin, dass ein Notfallzugriff technisch so einfach wie möglich zu gestalten sei. Der Kanton *TI* bezweifelt, dass die Anforderung einer schriftlichen Begründung und allfälliger Absicherungen eines Notfallzugriffes mit Passwort und Codes praktikabel sei. Dementsprechend müsse der Zugriff auf die Daten vereinfacht werden, bspw. mittels vorgegebener Antworten, die bestätigt werden müssten. Während sich das *LUKS* ebenfalls für eine nachträgliche statt vorgängige Begründung ausspricht und die *Insel* konkret die Streichung des Wortes „vorgängig“ fordert, begrüsst die *SPO*, dass ein Zugriff in medizinischen Notfällen vorgängig begründet und mit einer manuellen Interaktion abgesichert werden muss. Ähnlich wie die *SPO* bezeichnet die *FRC* eine kurze, vorgängige Begründung bei einem Notfallzugriff als notwendig.

Die *SMCF* macht einen konkreten Vorschlag, wie der Absatz 5 zu formulieren sei: „En cas d’urgence médicale, […] Ils doivent pouvoir motiver cet accès a posteriori“. Die *Tessaris* schlägt folgenden Wortlaut vor: „[…] auf die Vertraulichkeitsstufen „medizinische Daten“ und „sensible Daten“ zugreifen. Sie müssen die Begründung für einen solchen Zugriff im elektronischen Patientendossier in textlicher Form festhalten“. Die *IG eHealth* und *PH CH* würden den Absatz 5 mit folgendem Text bevorzugen: „In medizinischen Notfallsituationen können Ärzte auf die die Vertraulichkeitsstufe „medizinische Daten“ zugreifen. Sie müssen einen solchen Zugriff vorgängig durch eine Willensbekundung bestätigen. Die Willensbekundung 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. *Pharmasuisse* macht ebenfalls einen konkreten Formulierungsvorschlag: „[…] Gesundheitsfachpersonen auf sämtliche Vertraulichkeitsstufen zugreifen, sofern sie vom Patienten nicht generell vom Zugriff ausgeschlossen wurden. Sie müssen […]“. *CURAVIVA* und der *Insos* weisen darauf hin, dass es an Klarheit in Bezug auf den Zusammenhang von Absatz 5 mit Artikel 3 Buchstabe b in fine EPDV und das entsprechende Rangverhältnis fehle. Sie schlagen folgenden zusätzlichen Satz am Ende des Absatzes 5 vor: „Artikel 3 Buchstabe b in fine bleibt vorbehalten“. Der *VLSS* empfiehlt, dass in Absatz 5 vorgesehen wird, dass im Notfall auch der Zugang zu „sensiblen Daten“ besteht, ausser die / der betreffende Patientin / Patient dies gemäss Artikel 3 Buchstabe c auf „medizinische Daten“ oder auf „nützliche Daten“ eingeschränkt hat. Die *KAeG SG*, der *BüAeV*, die *GAeSO* und die *KKA* wünschen für Absatz 5 folgenden Zusatz: „Die Stammgemeinschaft stellt sicher, dass die Information über den Zugriff der Patientin oder dem Patienten auf der von ihr bzw. ihm vorgängig gewählten Zustellungsart erfolgt. Hat die Patientin oder der Patient keine Zustellungsart gewählt, erfolgt die Mitteilung der Information per

[16] GE, VS, VD, JU, FR, NE

Einschreiben“. Zudem fordern der *BüAeV*, die *GAeSO* und die *KKA* eine nähere Definition von medizinischen Notfällen und schlagen daher einen zusätzlichen Absatz für Artikel 5 mit folgendem Inhalt vor: „Medizinische Notfälle sind Fälle, bei welchen die Patientin oder der Patient infolge eines Unfalls oder infolge einer Krankheit dringend medizinischer Hilfe bedarf“.

Art. 3 Optionen der Patientinnen und Patienten

Die Patientin oder der Patient kann:

a. festlegen, dass die Zugriffsrechte nach Artikel 2 Absatz 1 nach sechs Monaten erlöschen;

b. das Zugriffsrecht für medizinische Notfallsituationen auf die Vertraulichkeitsstufe «nützliche Daten» einschränken, um die Vertraulichkeitsstufe «sensible Daten» erweitern oder vollständig ausschliessen;

c. festlegen, welche Vertraulichkeitsstufe neu eingestellten Daten zugewiesen wird;

d. einzelne Gesundheitsfachpersonen vom Zugriff auf ihr oder sein elektronisches Patientendossier ausschliessen;

e. die Information nach Artikel 8 Buchstabe f deaktivieren;

f. festlegen, dass Gesundheitsfachpersonen, die in eine Gruppe von Gesundheitsfachpersonen eintreten, nicht automatisch das mit der Gruppe verbundene Zugriffsrecht erhalten;

g. eine Stellvertretung benennen;

h. Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft dazu ermächtigen in ihrem oder seinem Namen Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen; dabei können diese höchstens die Zugriffsrechte zuweisen, die sie selber besitzen.

HIN wiederholt die bereits beschriebenen Bemerkungen zu Artikel 1. 9 Stellungnehmende[17] wiederholen zudem ihre Forderung zur Aufnahme einer Regelung betreffend urteilsunfähigen Personen und Kindern aus Artikel 2, für was sich auch der Kanton *SZ* ausspricht. Hinsichtlich urteilsunfähiger Personen schliesst sich auch der Kanton *BE* diesem Kommentar an. Der Kanton *ZG* und der *ZAD* weisen, wie bereits bei Artikel 2, darauf hin, dass auch eine Regelung für die verstorbenen Personen aufzunehmen sei. Die *FMH* wiederholt zudem ihre einleitend zu den Artikeln 1 und 2 aufgeführte Stellungnahme.

Die *FRC* bezeichnet die Buchstaben d bis h ausdrücklich als gut. 6 Kantone[18] wünschen die Aufnahme eines Buchstaben i mit folgender Formulierung: „Introduire la notion de délégation temporaire d’un professionnel de la santé à un autre (en cas d’absence), sans qu’un patient n’ait à ajouter ce professionnel dans les droits d’accès. Ce mode serait activé par défaut. Proposer une option de désactivation par le patient pour cette fonction de délégation de professionnel de la santé à un autre“. Die *ASPS* und der *Spitex* schlagen an dieser Stelle die Schaffung einer Art Inhaltsverzeichnis mit Benennung aller im elektronischen Patientendossier gespeicherten Dokumenten vor, damit die Patientin / der Patient darüber informiert werden könne, ob noch weitere Dokumente für die entsprechende Behandlung relevant wären. Die *KAeG SG*, der *BüAeV*, die *GAeSO* und die *KKA* weisen darauf hin, dass im Zusammenhang mit ihrem Vorschlag zur Aufnahme eines zusätzlichen Artikels für die Erfassung eigener Daten, Artikel 3 folgendermassen angepasst werden müsse: „[…] Vertraulichkeitsstufe die von ihr oder ihm selber erfassten Daten zugewiesen wird und/oder welches Zugriffsrecht gelten soll oder aber das Zugriffsrecht vollständig ausschliessen“. Im Zusammenhang mit ihren Ausführungen in den Erläuterungen und der Anpassung von Artikel 2 werde zudem folgende Anpassung von Artikel 3 notwendig: „[…] einzelnen Gesundheitsfachpersonen untersagen, die Zugriffsrechte an Hilfspersonen zu delegieren“. Analog sei zudem Ziffer 6 TOZ zu erweitern resp. zu ergänzen. Die *PKS* machen darauf aufmerksam, dass die Optionen für die Erteilung oder den Entzug von Zugriffsrechten einen erheblichen Aufwand für die Gemeinschaften bedeuten und Blacklisting einzelner Gesundheitsfachpersonen nicht der heutigen Behandlungspraxis im Gesundheitswesen entspreche. Die *SMCF* weist darauf hin, dass die Vielfalt und Komplexität der Optionen die Vorteile des elektronischen Patientendossiers zunichtemache. Zugriffsrechte sollten daher möglichst ganzheitlich für das gesamte elektronische Patientendossier verwaltet werden.

[17] GDK, BL, GL, LU, OW, UR, NW, ZG, ZAD

[18] FR, NE, GE, VS, VD, JU

Buchstabe a: Die *privatim*, der *DSBAG*, der *KDSBSON* sowie der Kanton *FR* schreiben, dass aus „Privacy by Default"-Überlegungen der Zugriff in der Grundeinstellung nicht unbefristet erfolgen solle. Analog dem Kanton *ZG* schlagen sie folgenden Formulierungsvorschlag für Artikel 3 Buchstabe a vor: „a. einzelnen Gesundheitsfachpersonen unbefristete Zugriffsrechte einräumen". Der Kanton *ZG* empfiehlt seinerseits die Prüfung einer Befristung der Dauer der Zugriffsberechtigung in der Grundeinstellung. Gemäss der *K3*, dem *VZK* und dem *VAKA* mache eine zeitliche Restriktion wenig Sinn und sei in der Handhabung zu komplex. Der Zugriff solle entweder gelten, oder nicht gelten. Genau wie *die Integic* fordern sie die Streichung von Buchstabe a. Die *Integic* sieht alternativ zur Streichung jedoch die Möglichkeit, zeitliche Einschränkungen in anderen Intervallen zu vergeben. In dieser Form seien die Buchstaben a und f jedenfalls auch in der Umsetzung für Systemhersteller zu kompliziert. Für den *VGIch* ist nicht einleuchtend, weswegen die optionale Befristung der Zugriffsrechte auf 6 Monate begrenzt sein solle. Analog *H+* und der *Insel* wünschen sie eine Lockerung dieser Fixierung, damit die Patientin / der Patient die Zeitdauer der Befristung eigenständig festsetzen kann. Die *IG eHealth*, *PH CH* und die *Post* empfinden eine feste Dauer von 6 Monaten als zu starr. Sie weisen darauf hin, dass die Patientinnen / Patienten einer Gesundheitsfachperson evtl. das Recht für nur eine Konsultation erteilen möchten und empfehlen folgenden Zusatz zu Buchstabe a: „[…] Artikel 2 Absatz 1 nach maximal 6 Monaten erlöschen;". 10 Stellungnehmende[19] weisen darauf hin, dass die Festlegung der Fristen den Anbietern von Lösungen zum elektronischen Patientendossier überlassen werden solle und schlagen folgende Umformulierung von Buchstabe a vor: „[…] Artikel 2 Absatz 1 befristet gelten;". Der Kanton *TI* macht geltend, dass aus dem Buchstaben a nicht klar hervorgehe, ob auch andere Laufzeiten zulässig sind, was zu klären sei. Die *Tessaris* bezeichnen die Befristung auf 6 Monate als überdeterminiert und empfiehlt, dass die unter Artikel 2 definierten Zugriffsrechte nach einer während der Konsultation von der Patientin / dem Patienten festgelegten Dauer erlöschen. Der Kanton *FR* macht darauf aufmerksam, dass die Patientin / der Patient mittels eines Alarms über die Befristung und ihre Folgen informiert werden sollte und fordert zu diesem Zweck die Aufnahme eines zusätzlichen Artikels oder Absatzes in der Verordnung.

Die *FRC* bezeichnet die Möglichkeit der Patientin / des Patienten zur automatischen Löschung der Zugriffsrechte nach 6 Monaten wiederum als sehr gut.

Buchstabe b: *CURAVIVA* und *Insos* wiederholen ihre Stellungnahme zu Artikel 2 Absatz 5. *PharmaSuisse* empfiehlt - unter Voraussetzung der Annahme ihres Formulierungsvorschlags von Artikel 2 Absatz 5 - folgende Änderung von Artikel 3 Buchstabe b,: „[…] medizinische Notfallsituationen generell auszuschliessen". Im Falle der Ablehnung des Formulierungsvorschlags von Artikel 2 Absatz 5 solle Artikel 3 Buchstabe b folgendermassen lauten: „[…] medizinische Notfallsituationen nach entsprechender Aufklärung des Patienten durch eine Gesundheitsfachperson auf die Vertraulichkeitsstufe […]". Der *Spitex* und die *ASPS* sprechen sich dafür aus, dass die Patientinnen / Patienten aktiv bestätigen müssen, falls bei einem Notfall die sensiblen Daten nicht angezeigt werden sollen. Die Standardeinstellung soll dementsprechend die „sensible Daten" beinhalten. Zudem sei eine automatische Notifikation über den erfolgten Notfallzugriff sinnvoll. Die *Tessaris* schreibt, dass Artikel 3 Buchstabe b unter Berücksichtigung ihres Formulierungsvorschlages zu Artikel 5 Absatz 2 zu streichen sei. Die *FRC* gibt zu bedenken, dass ein vollständiger Ausschluss des Zugriffsrechts für medizinische Notfälle ziemlich gefährlich sein könne. Für den Kanton *AG* wäre ein Ausschluss des Notfallzugriffs durch die Patientin / den Patienten heikel, wenn dieser oder diese bei der Vornahme der Einstellung nicht urteilsfähig wäre. Es sei wichtig, in den entsprechenden Erläuterungen den Bezug zum Kindes- und Erwachsenenschutzrecht herzustellen. Der *HÄ CH* und die *ÄTG* sehen den Sinn in Buchstabe b nicht und fordern dessen Streichung. Gemäss der *STSAG* sei auch bezüglich dieses Artikels klarzustellen, dass die Patientin / der Patient die Verantwortung für Behandlungsfolgen, welche aufgrund nicht verfügbarer Informationen entstehen könnten, zu tragen habe. Als Alternative solle in den Grundeinstellungen des elektronischen Patientendossiers sichergestellt werden, dass im Notfall auf alle Informationen zugegriffen werden kann.

Buchstabe c: Die *Tessaris* fordert die ersatzlose Streichung von Artikel 3 Buchstabe c, was sich aus der

[19] GDK, BL, GL, LU, OW, UR, AR, TG, BS, SZ

vorgeschlagenen Einleitung zu Artikel 1 ergebe. Der *HÄ CH* und die *ÄTG* bezeichnen diese Bestimmung als heikel und wünschen keine Wahlmöglichkeit. Mit Bezug auf ihren Kommentar zu Artikel 1 fordern sie per Default die Zuweisung zu medizinischen Daten.

Buchstabe d: Gemäss *H+*, dem *HÄ CH* und der *ÄTG* sollte der Notfallzugriff durch eine Fachperson trotz allgemeiner Sperre durch die Patientinnen / Patienten gewährt werden können. Ähnlich fordert der *VGIch*, dass die Patientin / der Patient die Möglichkeit haben sollte, Gesundheitsfachpersonen auszuschliessen und diesen doch den Notfallzugriff zu erlauben. Dieser Ansicht ist auch der Kanton *BS* und macht folgenden Formulierungsvorschlag: „[…] ausschliessen. Sie oder er kann ausgeschlossenen Gesundheitsfachpersonen das Zugriffsrecht für medizinische Notfallsituationen erteilen". Der *KSSG* ist der Meinung, dass der Buchstabe d mündlich gemachten Aussagen widerspreche, dass nicht alle Gesundheitsfachpersonen den Patientinnen / Patienten präsentiert werden müssen. Wenn tatsächlich eine Einschränkung der nach aussen präsentierten Gesundheitsfachpersonen möglich sein solle, sei Buchstabe d folgendermassen zu präzisieren: „d. einzelne der nach aussen sichtbaren Gesundheitsfachpersonen […]". Die *Tessaris* wünscht die ersatzlose Streichung von Artikel 3 Buchstabe d und verweisen auf die Stellungnahme zu Artikel 2 Absatz 3.

Buchstabe e: Der *VAKA* schreibt, dass bei Buchstabe e, wie in Artikel 2, von einem Standard auszugehen sei und nur effektive Ausnahmen möglich seien. Er schlägt Anpassungen aufgrund der Wertigkeit von Standard und Ausnahmen vor. Aufgrund ihrer Forderung, den Buchstaben f von Artikel 8 zu streichen, sei gemäss 6 Kantonen[20] folglich auch der Buchstabe e von Artikel 3 zu entfernen. Die *IG eHealth* und *PH CH* machen darauf aufmerksam, dass durch die aktuelle Regelung bei manchen Patientinnen / Patienten eine nicht zweckmässige Informationsflut entstehen könne. Deshalb sei Buchstabe e folgendermassen anzupassen: „e. kann jederzeit die aktuelle Zusammensetzung einer Gruppe von Gesundheitsfachpersonen abrufen". Die *Post* beschreibt die grosse Menge an Notifikationen aufgrund laufender Mutationen ebenfalls als Überflutung und fordert, wie auch der Kanton *ZG*, den Wechsel von „Opt-out" zu „Opt-in". Ähnlich empfiehlt die *Tessaris*, dass Patientinnen / Patienten verlangen müssen, dass sie über den Ein- oder den Austritt von Gesundheitsfachpersonen in eine bzw. aus einer Gruppe von Gesundheitsfachpersonen informiert werden. Der *Spitex* und die *ASPS* sprechen sich ebenfalls dafür aus, dass die Patientinnen / Patienten aktiv bestätigen müssen, dass sie über Neueintritte von Gesundheitsfachpersonen informiert werden wollen. In Buchstabe e sei dementsprechend das Wort „deaktivieren" mit „aktivieren" zu ersetzen. Die *K3* und der *VZK* erachten es aus Datenschutzgründen als nicht verantwortbar, dass Patientinnen / Patienten über ihr elektronisches Patientendossier alle Gesundheitsfachpersonen einer Gesundheitseinrichtung abfragen können, auch wenn diese nicht auf das eigene elektronische Patientendossier zugegriffen haben. Der Buchstabe e sei deshalb zu streichen.

Buchstabe f: Der *VGIch* wiederholt an dieser Stelle seinen Kommentar zu Artikel 2 Absatz 4 betreffend der Gruppenthematik und der *KDSBSON*, der *DSBAG* sowie die *privatim* ihre Stellungnahme, ebenfalls zu Artikel 2 Absatz 4, betreffend der „Opt-out"-Möglichkeit. Der *SBK*, der *SVBG* und *SWOR* erachten es als möglich, dass diese Bestimmung zu Umsetzungsschwierigkeiten in grösseren Organisationen führen könnte, weisen aber darauf hin, dass den Patientinnen / Patienten dieses Recht zugestanden werden müsse.

6 Kantone[21] sind der Meinung, dass eine Patientin / ein Patient weder die Möglichkeit erhalten sollte, Rechte von Gesundheitsfachpersonen, welche diese durch ihren Eintritt in eine Gruppe erhalten, zu ändern, noch einzelne Gesundheitsfachpersonen im Sinne einer „black-list" auszuschliessen. Die *Insel* weist darauf hin, dass der Ausschluss von einzelnen Personen innerhalb eines Spitals impraktikabel und in Primärsystemen kaum durchsetzbar sei. Im Falle eines notwendigen Notfallzugriffs sei dies zudem wohl auch nicht im Interesse der Patientin / des Patienten. Die *K3* und der *VZK* bemängeln die Praktikabilität im Spital ebenfalls. Wie auch die *Post* machen sie darauf aufmerksam, dass Zugriffsrechte für Gruppen vollständig sein müssen und alternativ lediglich eine oder mehrere einzelne Gesundheitsfachpersonen benannt werden könnten. Alles andere sei in den Spitälern nicht umsetzbar und führe

[20] FR, NE, GE, VS, VD, JU
[21] FR, NE, GE, VS, VD, JU

zu gefährlichen Situationen. Zudem müsse sichergestellt werden, dass Gesundheitsfachpersonen jederzeit sehen, ob sie vollen oder eingeschränkten Zugriff auf ein elektronisches Patientendossier haben. Für den *USB* ist die Möglichkeit der Patientin / des Patienten, neu in die Gruppe eintretende Gesundheitsfachpersonen generell vom Zugriff auszuschliessen, eine zu komplexe Aufgabe. Es müsse ausreichen, dass Gesundheitsfachpersonen auf die Ausschlussliste genommen werden können. Die Kantone *ZH*, *NW*, *ZG* und der *ZAD* betrachten Buchstabe f als nicht umsetzbar für grosse Leistungserbringer. Sämtliche Mitglieder einer Gruppe müssen Zugriff haben, andernfalls könnten lebensbedrohliche Situationen entstehen. Der *KSSG* plädiert dafür, dass neu eintretende Gesundheitsfachpersonen und Hilfspersonen automatisch die Berechtigung der Gruppe erben und das *LUKS*, die *Integic*, die *HL7*, *IHE* und *medshare* bemängeln, dass der Buchstabe f technisch und organisatorisch zu kompliziert in der Umsetzung sei. Die *Integic* schreibt zudem, dass nicht hervorgehe, ob die Patientin / der Patient aktiv darüber informiert wird, wenn eine Gesundheitsfachperson eine Weitergabe von Zugriffsrechten ausgeführt hat. Die *IG eHealth*, *PH CH* und die *Post* schreiben, dass eine Patientin / ein Patient entweder der Organisation und deren Fähigkeit zur Selbstorganisation, oder ansonsten Individuen vertrauen müsse. *SBC* bittet generell für eine Reduktion der Komplexität. Der *VAKA* spricht sich für die Zulassung von einer Vererbung der Zugriffsrechte aus und empfiehlt die Stärkung der Nutzung von primären Ausschlüssen und Einzelrechten statt dem Versuch, die Dynamiken von Gruppen zu managen.

24 Stellungnehmende[22] fordern eine alternativlose Streichung von Artikel 3 Buchstabe f. Die *Post* schlägt ebenfalls die Streichung vor, könnte sich als Alternative jedoch vorstellen, dass die Portale der Patientin / dem Patienten anbieten müssen, die Autorisierung an eine Gruppe zu erteilen oder die Mitglieder einer Gruppe zu kopieren. So sei für die Patientin / den Patienten immer klar, ob sie / er einzelne Individuen, oder aber eine ganze Gruppe autorisiert. Die *IG eHealth* und *PH CH* machen folgenden Vorschlag zur Umformulierung von Buchstabe f: „f. festlegen, dass keine Zugriffsrechte an Gruppen erteilt werden“. Die *Tessaris* fordert die Festlegung, dass Gesundheitsfachpersonen, die in eine Gruppe eintreten, erst nach namentlicher Bekanntgabe an die Patientin / den Patienten, das mit der Gruppe verbundene Zugriffsrecht erhalten. Die *SPO* fragt, ob die Stellvertretungen mit je eigener Identität erfolgen und wünschen eine verständlichere Formulierung.

Buchstabe g: Die *K3* und der *VZK* weisen darauf hin, dass es sehr häufig zu Stellvertreter-Regelungen kommen werde und die Verordnung insbesondere regeln solle, ab welchem Alter ein Kind selber ein elektronisches Patientendossier eröffnen oder die volle Verantwortung dafür übernehmen kann. Ähnlich macht der *VGIch* darauf aufmerksam, dass der Status von Kindern bzw. die Zugriffsrechte im Zusammenhang mit Sorgerecht nicht geklärt sei. Für die *IG eHealth*, *PH CH*, den Kanton *ZG* und die *Post* greife die Regelung zu kurz. Während die *IG eHealth* und *PH CH* die Klärung wünschen, wie bei einem Verlust der Handlungsfähigkeit zu verfahren ist, plädieren der Kanton *ZG* und die *Post* für eine Präzisierung zum Umgang mit Identifikationsmitteln, Vollmachten und Widerrufen.

Der Kanton *TI* wünscht die Definierung des Begriffes „Stellvertretung“, oder alternativ die Angabe, dass auf die „therapeutische Vertretung“ oder die „zur Vertretung bei medizinischen Massnahmen berechtigte Person“ gemäss Artikel 377 ZGB Bezug genommen werde. *Senesuisse* bezeichnet die Regelung der Rechte von Stellvertretern als unnötig und missglückt. Dies sei in Artikel 377 Buchstabe f ZGB viel klarer und umfassend geregelt. Es könnte dementsprechend darauf verwiesen und evtl. ergänzt werden. *CURAVIVA* und der *Insos* weisen darauf hin, dass bei urteilsunfähigen Patientinnen / Patienten deren Stellvertretung dazu befugt sei, in allen Bereichen Entscheidungen zu treffen, in denen die Patientin / der Patient selbst entscheiden könnte, wenn sie bzw. er urteilsfähig wäre, insbesondere in Bezug auf medizinische Massnahmen. Nach einer angemessenen Aufklärung durch den Arzt und das Pflegepersonal könne die Stellvertretung einer Behandlung und insbesondere der Eröffnung eines elektronischen Patientendossiers zustimmen oder diese ablehnen. Die Stellvertretung tritt jedoch nur dann in Aktion, wenn sich die urteilsunfähige Patientin / der urteilsunfähige Patient nicht selbst in der Patientenverfügung zu der zu treffenden Entscheidung geäussert habe (Art. 377 und 378 ZGB). Diese Regelung sei

[22] FR, NE, Insel, Integic, HL7, IHE, KSSG, K3, VZK, LUKS, SBC, ZH, NW, ZG, ZAD, USB, GE, VS, VD, JU, HÄ CH, ÄTG, medshare, STSAG

klar und in sich vollständig. Sie erweitere auf harmonische Weise die Regelung zum elektronischen Patientendossier. In dieser Hinsicht ist Artikel 3 Buchstabe g überflüssig und darüber hinaus unvollständig. Da er jedoch nicht im Widerspruch zur Gesetzgebung für den Schutz urteilsunfähiger Personen stehe, könne er so beibehalten werden. Der *HÄ CH* und die *ÄTG* weisen darauf hin, dass der Buchstabe g für Patientinnen / Patienten formuliert wurde und wünschen sich Stellvertretungsregelungen auch für Gesundheitsfachpersonen, namentlich Hausärzte mit regionaler (Notfall-)Vertretung oder Gruppenpraxen.

Buchstabe h: Der *KDSBSON*, der *DSBAG*, die *privatim* sowie die Kantone *FR* und *AG* fragen, ob es zutreffend und gewollt sei, dass Zugriffsrechte nur an Gesundheitsfachpersonen innerhalb derselben Stammgemeinschaft weitergegeben werden können, nicht aber auch an Gesundheitsfachpersonen anderer Stammgemeinschaften und Gemeinschaften. Falls nicht, sollte der Verordnungstext entsprechend angepasst werden. Zusätzlich schlagen sie, wie auch der Kanton *ZG*, folgende Formulierung für Buchstabe h vor: „h. Gesundheitsfachpersonen dazu ermächtigen, in ihrem Namen Zugriffsrechte weiteren Gesundheitsfachpersonen zuzuweisen. Eine Gesundheitsfachperson kann höchstens jene Zugriffsrechte zuweisen, die sie selber besitzt. Die Gesundheitsfachperson hat die Patientin oder den Patienten über entsprechende Zuweisungen zu informieren." Der Kanton *BE* schlägt folgenden Zusatz vor: „Die Gesundheitsfachperson hat die Patientin oder den Patienten über entsprechende Zuweisungen zu informieren". Die *IG eHealth*, *PH CH* und die *Post* plädieren dafür, dass die Weitergabe von Rechten bei Delegationen eine Standardeinstellung sein sollte. Gemäss dem *IG eHealth* und *PH CH* sollte die Patientin / der Patient dies optional aber einschränken können und die *Post* empfiehlt die Klärung, wie weit die Berechtigungskette geht. Die *IG eHealth* und *PH CH* machen folgenden konkreten Formulierungsvorschlag: „h. kann die Weitergabe von Rechten an weitere Gesundheitsfachpersonen seiner Stammgemeinschaft verbieten oder auf die Weitergabe an maximal eine weitere Gesundheitsfachperson oder Gruppe einschränken. Die *Tessaris* schlagen folgenden Wortlaut von Buchstabe h vor: „[…] Zugriffsrechte weiteren ihr oder ihm bekannt gegebenen Gesundheitsfachpersonen […]". Für den *VGIch* ist der Zweck, die Notwendigkeit, Beispiele sowie Abläufe betreffend der Ermächtigung zur Weitergabe der Zugriffsrechte unklar. Sie fordern entweder die Streichung von Buchstabe h oder die Klärung. Für den Kanton *AG* erscheint die Ermächtigung einer Gesundheitsfachperson, ihr Zugriffsrecht an weitere Gesundheitsfachpersonen weiterzugeben sinnvoll. Es berge jedoch eine gewisse Gefahr für die Patientinnen / Patienten, weshalb sie nach Beispielen bitten. Der *HÄ CH* und die *ÄTG* fordern eine Regelung für Behandlungen ausserhalb der eigenen Stammgemeinschaft.

3.1.2 2. Kapitel: Patientenidentifikationsnummer

Art. 4 Format der Patientenidentifikationsnummer

[1] Die Patientenidentifikationsnummer ist elfstellig. Sie setzt sich zusammen aus einer Kontrollziffer und einer zehnstelligen Nummer. Diese darf für eine bestimmte, im Register der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) nach Artikel 71 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG) verzeichnete Person verwendet werden, jedoch keinerlei Rückschlüsse auf diese Person zulassen.

[2] Die Patientenidentifikationsnummer darf nur manuell erfasst werden, wenn eine Kontrollzifferprüfung durchgeführt wird. Das Eidgenössische Departement des Innern (EDI) legt die Vorgaben für den Aufbau der Patientenidentifikationsnummer und die Kontrollzifferprüfung fest.

Gemäss der *Insel* sei aus Spitalsicht schwer nachzuvollziehen, weshalb nicht die AHV-Nummer zur Identifikation der Patientinnen / Patienten verwendet werden dürfe und stattdessen eine separate Nummer von der zentralen AHV-Ausgleichsstelle generiert werden müsse. Mit Blick auf etablierte eHealth-Lösungen im Ausland sei es letztlich ein fragwürdiger, kostentreibender Faktor für die Schweiz. Die *STSAG* weist darauf hin, dass jede Patientin / jeder Patient nur eine PID erhalten solle, was festzuschreiben sei. Die *Bethesda* und die *RPB* wünschen, dass eine klare Regelung im Umgang mit Neugeborenen betreffend dem Zuweisungszeitpunkt zu einer eigenen elektronischen Patientendossier-PID erfolge. Sie sprechen sich dafür aus, dass möglichst früh ein elektronisches Patientendossier eröffnet werden kann, welches durch die Mutter oder den Vater als Stellvertreter geführt wird.

Absatz 1: Der *DSBAG*, *privatim* sowie die Kantone *ZG* und *SZ* schreiben, dass aus datenschutzrechtlicher Sicht zu begrüssen sei, dass die PID keinerlei Rückschlüsse auf die Person zulasse. Dem stimmen auch die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* zu. Für sie stellt sich dabei die Frage, ob und weshalb es notwendig sein solle, dass die PID bei der ZAS gespeichert wird. Es solle zudem vermieden werden, dass die ZAS eine PID einer bestimmten Person zuweisen kann. 7 Stellungnehmende[23] machen geltend, dass der Einsatz von internationalen Standards, wie den GS1-GSRN, einer isolierten Schweizer Lösung vorzuziehen wäre. *ICTS*, *IG eHealth* und *PH CH* macht folgenden Formulierungsvorschlag für Artikel 4 Absatz 1: „Die PID ist nach internationalen Standards für PID aufgebaut. Diese darf […]". *Stiftung refdata*, *GS1* und die *SGMI* schreiben, dass sich die Prüfziffer bei den GS1-GSRN auf dem Algorithmus Modulo-10, welcher auch für die Prüfzifferberechnung im aktuellen Entwurf vorgeschlagen ist, berechne. Die im Jahr 2015 CEN übernommene ISO „Technische Spezifikation 18530" illustriere, wie ein solcher Schlüssel (GSRN) aufgebaut sei und genutzt werden könne. Zusätzlich machen sie ein Beispiel, wie die GSRN aufgebaut ist und verweisen auf die Grafik dazu im Anhörungsdokument. *Economiesuisse* macht darauf aufmerksam, dass die hier vorgeschlagene Lösung verhindere, dass z.B. Grenzgänger ein elektronisches Patientendossier eröffnen können, was zu beheben sei.

Art. 5 Antrag auf Zuweisung der Patientenidentifikationsnummer

[1] Die Patientenidentifikationsnummer wird auf Antrag einer Stammgemeinschaft durch die ZAS vergeben.

[2] Die Stammgemeinschaft stellt der ZAS folgende Daten für die Vergabe der Patientenidentifikationsnummer zur Verfügung:

a. den Namen;

b. die Vornamen;

c. das Geschlecht;

d. das Geburtsdatum;

e. die Versichertennummer nach Artikel 50c AHVG

[3] Reichen die gemeldeten Daten für die Vergabe nicht aus, so kann die ZAS bei der Stammgemeinschaft zusätzliche Daten verlangen.

Die *Insel* wiederholt ihren Kommentar zu Artikel 4. Der *VAKA*[24] schlägt vor, dass der Stammgemeinschaft mutierte, demographische Daten automatisch und elektronisch gemeldet werden müssen. 6 Kantone[25] verlangen, dass aus Sicherheits- und Kostengründen die Benutzung der PID innerhalb der Gemeinschaft (in den Primärsystemen) möglich ist und die Identitäten der Patientinnen / Patienten in eindeutiger Art sichergestellt wird. Die Kantone *NE*, *GE*, *JU*, *VS* und *VD* fragen, was die Fristen und Kosten für die Erstellung einer PID und die anschliessende Eröffnung eines elektronischen Patientendossiers seien. Idealerweise sollte es in einem „Transaktionsmodus" möglich sein, eine PID zu erhalten und ein elektronisches Patientendossier direkt aus dem Primärsystem zu erstellen. Sie fordern, dass der Antrag für die Erstellung einer PID elektronisch und im Erstellungsprozess des elektronischen Patientendossiers verfügbar sein muss. Die PID müsse zudem sofort zur Verfügung stehen.

Absatz 1: Der *VAKA*, die *K3* und der *VZK* weisen darauf hin, dass gemäss diesem Text wohl ein Versicherungsstatus in der Schweiz für die Eröffnung eines elektronischen Patientendossiers nötig sei. Falls dies zutreffe, könnten Personen ohne AHV13 (z.B. Touristen, Diplomaten, Grenzgänger etc.) wohl kein Dossier eröffnen. Während die *K3* und der *VZK* die Prüfung dieser Thematik fordern, sprechen sich der *VAKA* sowie der Kanton *AG* für die Berücksichtigung möglichst aller Personengruppen bei der Vergabe der PID aus. Ähnlich verlangen die *Post* sowie die *H+*, dass PID auch für Personen ohne eine AHVN13 ausgelöst werden können. *H+* beantragen zudem, dass die Stammgemeinschaften für den Antrag auf Zuweisung der PID die Sedex-Übermittlungsplattform zur ZAS nutzen können. Nur so sei ein effizienter und bereits standardisierter elektronischer Meldeweg für diesen Prozess gewährleistet. Die *OFAC* fragt generell, was mit Patientinnen / Patienten geschieht, welche ein elektronisches Patientendossier eröffnen wollen, jedoch über keine AHVN13 verfügen. Die *IG eHealth* und *PH CH* schlagen folgenden Zusatz

[23] GS1, Stiftung refdata, SGMI, ICTS, IG eHealth, PH CH, economiesuisse

[24] Ohne RPB

[25] FR, NE, GE, JU, VS, VD

bei Artikel 5 Absatz 1 vor: „[...] vergeben. Die ZAS stellt sicher, dass auch nicht obligatorisch Versicherte nach Art. 1 AHVF im zentralen Versichertenregister ohne AHV13 geführt werden können und dass die Stammgemeinschaften für die Personen eine PID beantragen dürfen“. Die *K3* und der *VZK* fordern, dass der Prozess gemäss Absatz 1 möglichst einfach gehalten wird. Die *ASPS* und der *Spitex* schlagen eine Vergabe der PID an alle Personen mit einer AHV-Nummer vor, da dies die Registrierung vereinfachen würde. Den Leistungserbringern, die via Stammgemeinschaft ein neues elektronisches Patientendossier anlegen resp. eine PID anfragen, sollen keine zusätzlichen Kosten entstehen.

Absatz 2: *Santésuisse* plädiert dafür, dass neben den Stammgemeinschaften auch der Identity-Provider die in Absatz 2 genannten Daten dem ZAS übermitteln darf. Die *BRH* ist der Ansicht, dass die AHV-Nummer als Teil der PID den Datenschutz unterminiere und fordert, dass die Patientenidentität und Versichertenidentität getrennt sein müssen. *PharmaSuisse* gibt zu bedenken, dass gemäss Artikel 4 Absatz 1 die PID keinerlei Rückschlüsse auf die Person zulassen dürfe. Jedoch könnte von einer Stammgemeinschaft im Zuge des Antrags auf Zuweisung der PID eine solche Verknüpfung mit der AHV-Nummer gemacht werden. Die Frage stelle sich, ob im Regelwerk eine entsprechende Geheimhaltungsklausel vorgesehen sei.

Absatz 3: Die *K3* und der *VZK* betrachten es als fraglich, ob die Stammgemeinschaft für Nachfragen nicht über weitere Daten zum Nutzer eines elektronischen Patientendossiers verfügen müsse. Sie schlagen vor, dass die ZAS der Stammgemeinschaft automatisch Mutationen von Adressdaten, Namen etc. melden solle. 6 Stellungnehmende[26] fragen, um welche Daten es sich handle und wünschen deren Präzisierung. Die *medshare* bittet zudem generell um eine Definierung des Begriffes „Daten“. Dieser werde regelmässig im gesamten Verordnungswerk verwendet, teilweise jedoch mit unterschiedlicher Interpretation. Die *Tessaris* geht davon aus, dass durch Absatz 3 u.a. die Fälle erfasst werden, in welchen Personen, die sich in der Schweiz (z.B. als Touristen) aufhalten, nicht über eine Versichertennummer nach Artikel 50 Absatz C AHVG verfügen. Das *KSSG* weist darauf hin, dass der Service zur Einholung von Zusatzinformationen beschrieben werden müsse und ein manueller Antrag diesbezüglich zu aufwändig sei.

Art. 6	Abfrage der Patientenidentifikationsnummer
Gemeinschaften und Stammgemeinschaften können die Patientenidentifikationsnummer bei der ZAS über ein elektronisches Abrufverfahren abfragen.	

Die *ASPS* und der *Spitex* wiederholen ihre Stellungnahme von Artikel 5. Die *HL7*, *IHE* und die *Integic* wünschen eine Klärung, welche Daten für die Anfrage nötig seien und schlagen die Daten gemäss Artikel 5 Absatz 2 vor. Die *K3* und der *VZK* weisen darauf hin, dass die Abfrage auch für Leistungserbringer und Gesundheitsfachpersonen ermöglicht werden solle. Andernfalls könnten im Notfall Daten, aufgrund des fehlenden Zugriffs zum Dossier, u.U. nicht aufgefunden werden. Die *Post* macht darauf aufmerksam, dass die PID auch für die Kommunikation zwischen Leistungserbringer und Patientin / Patient genutzt werden könne. Die PID solle darum ein Leben lang gültig und gleich sein. Es sei zu prüfen, ob weitere Verwendungszwecke der PID möglich sind und diese entsprechende Rechtsgrundlagen in der EPDV benötigen.

Art. 7	Annullierung
[1] Wird das elektronische Patientendossier aufgehoben, so wird die Patientenidentifikationsnummer in der Identifikationsdatenbank der ZAS annulliert.	
[2] Eine annullierte Patientenidentifikationsnummer darf nicht erneut vergeben werden.	

Das *KSSG* weist analog der Stellungnahme in Artikel 5 darauf hin, dass dieser Service im Detail zu beschreiben sei. Die *VAKA* wiederholt an dieser Stelle die Stellungnahme von *Bethesda* und dem *RPB* aus Artikel 4. *Lovis* macht geltend, dass die PID erhalten bleiben müsse und der Emittent die Einzigar-

[26] HL7, IHE, VAKA, Post, ZG, medshare

tigkeit der PID zu gewährleisten habe. Ähnlich fordern der Kanton *TI* und der *FMH*, dass Artikel 7 dahingehend zu ändern sei, dass die PID bei der Schliessung eines elektronischen Patientendossiers aufbewahrt und bei Bedarf der Wiedereröffnung der Patientin / dem Patienten erneut zugewiesen wird. Der Kanton *AG* macht unter Artikel 5 und 7 darauf aufmerksam, dass ein nicht unerheblicher Aufwand für die Stammgemeinschaft entstehe, wenn sie bei Widerruf des elektronischen Patientendossiers die Aufhebung der PID beantragen müsse. Die *medshare* weist an dieser Stelle darauf hin, dass ein elektronisches Patientendossier von der Eröffnung bis zum Tod der Patientin / dem Patienten gehöre. Aus diesem Grund habe niemand ausser sie / er das Recht, Daten zu löschen. Eine PID sei dementsprechend nur auf Wunsch der Patientin / des Patienten bei der ZAS aufzuheben. Im Falle der Aufhebung müsse sie zudem auch in allen MPI's gelöscht werden. 6 Kantone[27] machen geltend, dass die PID auch für die Kommunikation zwischen Gemeinschaften eigesetzt werden könne. Eine Patientin / ein Patient, welche / welcher umgezogen ist, könne bei zwei Stammgemeinschaften registriert sein. Eine PID dürfe zudem niemals annulliert werden. Es gingen die Übereinstimmungen der Identitäten im MPI der Stammgemeinschaft und dem MPI der Gemeinschaft verloren. Genau wie die AHVN13 grundsätzlich nicht mit der Person ändert, muss die PID nach der Aufhebung des elektronischen Patientendossiers behalten werden. Deren Beibehaltung ist die Basis für die Interoperabilität. Zudem müsse eine einzige PID mit einer einzigen AHV-Nummer übereinstimmen. Sie machen folgenden Formulierungsvorschlag für Artikel 7 Absatz 1: „[…] son numéro d'identification est conservé". Für Absatz 2 wünschen sie folgenden Wortlaut: „En cas de création ultérieure d'un nouveau dossier électronique du patient, le numéro d'identification initial dout être repris".

Absatz 1: Die *HL7*, *IHE*, die *BINT* und die *Integic* machen geltend, dass die elektronische Patientendossier-PID auch in allen MPI's gelöscht werden müsse. Sie empfehlen die Streichung dieses Artikels. Wenn das Konzept bleibe, müssten MPI, Reg. & Rep. bereinigt werden. Die *BINT* und die *Integic* fordern zudem, dass die Stammgemeinschaften alle zertifizierten Gemeinschaften und die ZAS über ein aufgehobenes elektronisches Patientendossier benachrichtigen müssen.

Absatz 2: Die *BINT* und die *Integic* plädieren dafür, dass Gemeinschaften und Stammgemeinschaften annullierte PID befristet bei der ZAS über ein elektronisches Abrufverfahren abfragen können. Die *Post* schlägt die explizite Erwähnung vor, dass Absatz 2 auch für die gleiche Patientin / den gleichen Patienten gilt. Die *ASPS* und die *Spitex* schlagen wiederum vor, dass bei einer Wiedereröffnung eines elektronischen Patientendossiers die „alte" PID aktiviert werden sollte. Die *BFH* erachtet es als ratsam, einen Absatz 3 einzufügen, in welchem spezifiziert wird, wie das Nummernmanagement aussieht, wenn nach der Annullierung erneut ein elektronisches Patientendossier eröffnet wird.

3.1.3 3. Kapitel: Gemeinschaften und Stammgemeinschaften

1. Abschnitt: Gemeinschaften

Art. 8 Verwaltung

Gemeinschaften müssen die ihnen angehörenden Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen verwalten. Dazu müssen sie insbesondere:

a. deren Eintritt und deren Austritt regeln;

b. die Gesundheitsfachpersonen identifizieren;

c. die Aktualisierung der Daten im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 sicherstellen;

d. sicherstellen, dass Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier nur gültige Identifikationsmittel verwenden, die von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurden;

e. sicherstellen, dass die Zusammensetzung der Gruppen von Gesundheitsfachpersonen für Patientinnen und Patienten jederzeit nachvollziehbar ist;

[27] FR, GE, VS, VD, JU, NE

f.	die Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informieren.

Der *VGIch* wiederholt an dieser Stelle seinen Kommentar zu Artikel 2 Absatz 4 sowie Artikel 3 Buchstabe f betreffend der Gruppenthematik. 16 Stellungnehmende[28] kritisieren den hohen administrativen Aufwand, welcher im Zuge der Bestimmungen von Artikel 8 entstehe. Der *VAKA* fordert eine Überarbeitung zur Reduktion des Aufwandes. *Physioswiss*, der *SBK*, die *SWOR* und der *SVBG* regen an, dass die Prozesse frühzeitig geregelt und praxistauglich implementiert sein müssen. Zusätzliche Ressourcen müssten dafür bereitgestellt werden. *PharmaSuisse* weist darauf hin, dass das Apothekenteam von Patientinnen / Patienten als Gruppe für den Zugriff auf das elektronische Patientendossier berechtigt werden können sollte, da sonst Abläufe für banale Team-Aktivitäten extrem verkompliziert würden. Der Kanton *TI* unterstreicht die Wichtigkeit, dass Patientinnen / Patienten einer Gruppe von Gesundheitsfachpersonen, die untereinander zusammenarbeiten, Zugriff auf ihre Daten gewähren können und verweisen auf die praktischen Erfahrungen aus dem Projekt „reTIsan".

Für *IG eHealth* und *PH CH* stellt sich die Frage, wie sichergestellt werden soll, dass die Patientin / der Patient die Identität der Hilfspersonen auch über die verschiedenen Gemeinschaften / Stammgemeinschaften hinweg kennt und sieht, wem sie / er Zugriff erteilt. Sie machen einen konkreten Formulierungsvorschlag für Artikel 8: „[…] Gesundheitsfachpersonen, Hilfspersonen und Gruppen von Gesundheitsfachpersonen verwalten. […]". *HIN* geht, gestützt auf die Ausführungen auf Seite 15 der Erläuterungen zur EPDV sowie der Botschaft zu Artikel 3 EPDG davon aus, dass eine Gesundheitsfachperson die Bearbeitung des elektronischen Patientendossiers an ihre Hilfspersonen delegieren könne, ausser dies wäre von der Patientin / dem Patienten ausdrücklich untersagt worden. Sie empfehlen, dass die Patientin / der Patient bei der Einwilligung der Erfassung ihrer / seiner Daten im elektronischen Patientendossier die von ihm berechtigten Gesundheitsfachpersonen ermächtigen müsse, nach dessen Ermessen Hilfspersonen beizuziehen. *HIN* verweist auf ihre ergänzenden Punkte zu den Artikeln 2 und 3 und wünscht, falls diese nicht berücksichtigt würden, eine klarere Definition, welche Berufe / Ausbildungen unter den Begriff „Gesundheitsfachperson" fallen. Zudem macht *HIN* folgende Formulierungsvorschläge für zusätzliche Buchstaben in Artikel 8: „g. sicherstellen, dass die zugeordneten Hilfspersonen von Gesundheitsfachpersonen für Patientinnen und Patienten jederzeit nachvollziehbar sind;" sowie „h. die Patientinnen und Patienten über das erstmalige Zuordnen von Hilfspersonen von Gesundheitsfachpersonen informieren". Gemäss dem *KSSG* sei Artikel 8 zu ergänzen, damit sinngemäss folgende Forderungen erfüllt seien: Das BAG bezeichnet die Berufsgruppen, die als Gesundheitsfachpersonen gelten. Der Kanton bezeichnet die eidgenössischen oder kantonalen Register, mit welchen die Zulassung der Gesundheitsfachpersonen überprüft werden muss. Alle nicht als Gesundheitsfachpersonen explizit bezeichneten Berufsgruppen gelten als Hilfspersonen im Sinne der TOZ 1.3". Ausserdem solle folgender, zusätzlicher Buchstabe ergänzt werden: „Das BAG kann Gemeinschaften auf Antrag erlauben, aus Gründen der Übersichtlichkeit für die Patientinnen oder die Patienten nur einen Teil der GFS nach aussen zu publizieren".

Die *STSAG* macht darauf aufmerksam, dass die Zwei-Faktor-Authentifizierung kaum praktikabel sei. Es solle die Aufnahme einer HIN-Access-Gateway ähnlichen Infrastruktur als akzeptiertes Äquivalent für den authentifizierten Zugriff geprüft werden. Bezüglich der Verwaltung von Gesundheitsfachpersonen fordern der *HÄ CH* und die *ÄTG* eine Vereinfachung. Sie schlagen eine Ausgestaltung dieser Steuerung in 2 Modi vor. Einen Professional-Mode für alle, die sich hier ausgiebig vertiefen und alles selbst steuern und einstellen wollen sowie einen Easy-Mode, der mit einem „Mausklick" per Default alle Einstellungen in einer (allenfalls noch zu diskutierenden) vernünftigen und eher liberalen Art hinterlegt.

Die Kantone *NW*, *ZG*, *ZH* sowie der *ZAD* sind der Ansicht, dass keine indirekten Bestimmungen zu verwenden seien, sondern direkt geregelt werden solle, was die Gemeinschaften tun müssen. Die Kanton *ZG*, *ZH* und der *ZAD* machen folgenden Formulierungsvorschlag für Artikel 8 inkl. Anmerkungen:

[28] ASPS, Spitex, Insel, VAKA, RPB, Physioswiss, PKS, SVP, SBK, SWOR, SVBG, Post, STSAG, HÄ CH, ÄTG

„Gemeinschaften verwalten die ihnen angehörenden Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen. Dabei gelten folgende Grundsätze:
a. Die Gemeinschaft regelt, wie Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen ihr beitreten oder sie verlassen [Was haben die Gemeinschaften genau zu regeln? Ist erforderlich, dass sie Ein- und Austritt regeln? Braucht es diese Bestimmung wirklich?];
b. Die Gemeinschaft identifiziert die Gesundheitsfachpersonen [Identifikationsmittel? Was genau muss die Gemeinschaft überprüfen? Wann identifiziert sie?].
c. Die Gemeinschaft aktualisiert die Daten im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Art. 40.
d. Die Gemeinschaft lässt Zugriffe auf das elektronische Patientendossier nur zu, wenn dafür ein gültiges Identifikationsmittel verwendet wird, das von einem nach Art. 30 zertifizierten Herausgeber stammt.
e. Die Gemeinschaft informiert Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen."

Buchstabe b und c: Die *ASPS* und der *Spitex* weisen darauf hin, dass in der Schweiz bis heute kein umfassendes Register für Pflegefachpersonen existiere. Das Gesundheitsberufsgesetz sieht die Schaffung eines nationalen Registers zwar vor, da dieses anfangs 2017 jedoch kaum in Kraft sein werde, sei eine Übergangslösung wichtig. Die EPDV müsse ein vollständiges Register vorsehen oder einen Übergangsprozess definieren, damit auch Pflegefachpersonen in jedem Fall zertifiziert werden können. Der Eintrag in ein nationales Register solle zudem kostenlos sein und es müsse von einer unabhängigen Stelle betrieben werden. Ähnlich machen der *SBK*, der *SVBG*, die *SWOR* und die *H+* darauf aufmerksam, dass die eindeutige Identifikation der Gesundheitsfachpersonen, insbesondere im Bereich der Pflege, die Gesundheitseinrichtungen und Gemeinschaften vor grosse Herausforderungen stellen werde, weshalb ein vollständiges, nationales Berufsregister zur verlässlichen Identifikation unumgänglich sei. Die HL7, IHE, die *Integic* und die *medshare* schlagen folgende Präzisierung von Buchstabe b vor: „die Gesundheitsfachpersonen authentifizieren und eindeutig identifizieren". Für Buchstaben c wünschen sie zudem die Festlegung einer Periodizität. Der Kanton *AG* fordert die Klärung der Identifikation der Hilfspersonen und eine Präzisierung der zugriffsberechtigten Hilfspersonen.

Buchstabe d: Der *VGIch* und die *Insel* geben zu bedenken, dass sich ein Spital als Herausgeber von Identifikationsmittel gemäss diesem Artikel zertifizieren lassen bzw. qualifizierte Signaturen für angeschlossene Primärsysteme einsetzen müsste. Die *Insel* fordert die ersatzlose Streichung von Buchstabe d und der *VGIch* weist darauf hin, dass die Wahl für geeignete Verfahren des Identity Managements von Spitalmitarbeitenden ausschliesslich bei den Spitälern liege. Gemäss dem *KSSG* sei in den TOZ unter 1.4 zu präzisieren, dass die Identität der Gesundheitsfachpersonen und der Hilfspersonen elektronisch gesichert abgelegt und mit einer starken Authentifizierung für den Zugriff auf das elektronische Patientendossier abgerufen werden könne.

Der *HÄ CH* und die *ÄTG* schlagen vor, den Zugriff auf das Primärsystem weiterhin, wie bisher allgemein üblich, einstufig zu belassen und die zertifizierten, zweistufigen Sicherheitsmerkmale erst sekundär dann zum Einsatz zu bringen, wenn das Primärsystem mit dem elektronische Patientendossier in Verbindung tritt, um Daten abzurufen oder dort abzulegen. Es sei auch vorstellbar, dass nur gewisse Stationen innerhalb einer Praxis mit dem elektronischen Patientendossier in Kontakt treten und dort entsprechende Sicherheitsmerkmale installiert werden.

Buchstabe e: Gemäss 6 Kantonen[29] sollten die Patientinnen / Patienten die Zusammensetzung der Gruppen nicht in Echtzeit abfragen können, dafür jederzeit (über die Zugriffsprotokolle) Einsicht haben, welche Gesundheitsfachperson aus welcher Gruppe ihre / seine Daten abrief. Artikel 8 Buchstabe e sei zu streichen. Gegen eine Echtzeitaktualisierung und für die Streichung von Buchstabe e spricht sich auch der Kanton *TI* aus. Ebenfalls die Streichung von Buchstabe e wünschen die *STSAG*, der Kanton *ZG*, die *K3* und der *VZK*. Die *BFH* schlägt als erste Priorität vor, Gruppen pragmatisch, so wie es heute bereits der Fall sei, auf den Chefarzt „und sein Team" zu reduzieren. Zweite Priorität resp. falls auf Buchstabe e beharrt werde, solle der Patientin / dem Patienten u.a. klar aufgezeigt werden, dass auch

[29] FR, GE, VS, VD, JU, NE

die Gesundheitsfachpersonen mit verweigerten Zugriffsrechten über ihr klinisches (Primär-)System Einsicht in die Daten erhalten. Der *KSSG* bemängelt, dass die Nachvollziehbarkeit für die Patientinnen / Patienten durch den Ausschluss von Hilfspersonen nicht gegeben sei. Dadurch ergebe sich ein Widerspruch durch TOZ 1.3.2.2. Falls dies tatsächlich erforderlich sei, sollen auch Hilfspersonen im HPD geführt und mit den zentralen Diensten synchronisiert werden. Dies sei jedoch nicht in ihrem Sinne. Es wird eine Berechtigungssteuerung auf Gruppen- oder Organisationsebene gefordert und einzelne Gesundheitsfachpersonen seien explizit auszuschliessen. Der *SBK*, der *SVBG* und die *SWOR* betrachten die Informationsflut, welche entstehe, wenn die Patientinnen / Patienten über personelle Wechsel im Behandlungsteam informiert werden, als kritisch. Zudem sei diese Transparenz auch für die Gesundheitsfachpersonen kritisch zu betrachten. Der *VGIch* wünscht die Nennung der Kriterien, an welchen sich die Verhältnismässigkeit der Gruppe messe. Der *HÄ CH* und die *ÄTG* bezeichnen die Verwaltung von Gesundheitsfachpersonen (Bst. e und f) als zu komplex. Sie befürchten eine Überforderung der Patientinnen / Patienten und es bestehe die Gefahr, dass die nötige Ärztin / der nötige Arzt doch nicht zugriffsberechtigt sei.

Buchstabe f: 16 Stellungnehmende[30] weisen darauf hin, dass eine aktive Information bei Änderungen von Gesundheitsfachpersonen in den Gruppen, vor allem bei grösseren Institutionen, zu einer unnötigen Informationsflut führe. Ebenfalls 16 Stellungnehmende[31] fordern dementsprechend die Streichung von Buchstabe f. Die *Insel*, die *K3,* der *VZK* und der *LUKS* geben als Grund dafür ausserdem den Konflikt mit dem Datenschutz des Spitalpersonals an. Der *KSSG*, die *SGMI*, die *FMH* und der *LUKS* beantragen die Streichung der aktiven Informationspflicht. Analog der *Insel* reiche es, wenn die Patientin / der Patient diese Informationen bei Bedarf abrufen könne. *SCH* schlägt folgenden Zusatz für Buchstabe f vor: „die Patientinnen und Patienten mittels einer Opt-in-Option über die Eintritte […]". *Economiesuisse*, die Kantone *ZG*, *NW*, *ZH* sowie der *ZAD* sprechen sich ebenfalls dafür aus, die Information auf eine Opt-in-Option zu beschränken. Die *HL7*, *IHE* und die *Integic* schreiben, dass Ein- und Austritte von Gesundheitsfachpersonen nur über die Gruppen, welche die Patientin / der Patient aktuell berechtigt hat, zu senden seien. Sie sind der Meinung, dass die Möglichkeit zum Muting solcher Meldungen die Akzeptanz erheblich unterstützen dürfte. Die *Integic* empfiehlt zudem, die Aufbewahrung der Protokollierung nach Austritt zu konkretisieren. Die *PKS* und die *SVP* empfinden es als ausreichend, wenn Patientinnen / Patienten die tatsächlich erfolgten Zugriffe auf das elektronische Patientendossier jederzeit nachvollziehen können. Das ganze Spital sollte dabei als Gruppe für den Zugriff berechtigt sein. Der *VGIch* schreibt, dass der Prozess „Eintritt von Gesundheitsfachpersonen" für alle in einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen ausgelöst werden müsse. Gemäss den Erläuterungen sei es möglich, dass den Gesundheitseinrichtungen der Eintrittsprozess delegiert werden könne. Die Bestimmung müsse dahingehend interpretiert werden, dass die Gesundheitseinrichtungen selbst bezeichnen können, wer aktiv eintritt. Die TOZ sei dahingehend zu ändern.

Art. 9 Datenhaltung und Datenübertragung

[1] Gemeinschaften müssen sicherstellen, dass:

a. die von den Gesundheitsfachpersonen im elektronischen Patientendossier erfassten Daten nach 10 Jahren vernichtet werden;

b. bei einer Aufhebung des elektronischen Patientendossiers nach Artikel 20 Absatz 1 sämtliche Daten vernichtet werden;

c. Daten des elektronischen Patientendossiers nur in Ablagen gespeichert werden, die ausschliesslich dafür vorgesehen sind.

[2] Sie haben auf Verlangen der Patientin oder des Patienten:

a. bestimmte auf diese oder diesen bezogene Daten im elektronischen Patientendossier nicht zu erfassen;

b. Daten nach Absatz 1 weitere 10 Jahre verfügbar zu machen;

c. bestimmte auf diese oder diesen bezogene Daten aus dem elektronischen Patientendossier zu vernichten.

[30] AG, ASPS, Spitex, FR, GE, VS, VD, JU, NE, Insel, KSSG, FMH, SCH, economiesuisse, LUKS, Post, TI

[31] FR, GE, VS, VD, JU, NE, Insel, K3, VZK, LU, SCH, TI, STSAG, NW, ZH, ZAD

[3] Das EDI legt die weiteren Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers fest. Es regelt insbesondere:

a. die Umsetzung der Artikel 1 und 2 Absatz 5;

b. die zu verwendenden Metadaten;

c. die zu verwendenden Austauschformate;

d. die zu verwendenden Integrationsprofile;

e. die Vorgaben betreffend die Protokolldaten.

[4] Das EDI kann bestimmen, dass die Vorgaben nach Absatz 3 in der Originalsprache veröffentlicht werden und auf eine Übersetzung in die Amtssprachen verzichtet wird.

[5] Das Bundesamt für Gesundheit (BAG) kann die Vorgaben nach Absatz 3 dem Stand der Technik anpassen.

Der *HÄ CH* und die *ÄTG* fragen, ob bei einem Nicht-Zugriff auf ein Dossier auch rechtliche Schritte eingeleitet resp. daraus abgeleitet (z.B. Unterlassung) werden können und bitten um die Erarbeitung eines juristischen Gutachtens zur Klärung der derzeit für Patientinnen / Patienten und Gesundheitsfachpersonen unklaren Fragestellung. Die *PKS* und die *SVP* kritisieren, dass die Bestimmungen, welche die Datenspeicherung betreffen, aufwändig umzusetzen seien, da sie nicht den heutigen Prozessen in Spitälern entsprechen würden. Insbesondere die separate Datenspeicherung führe zu keinem Mehrwert für die Patientinnen / Patienten, dafür zu erheblichen Mehrkosten für die Gemeinschaften.

Absatz 1: Die *IG eHealth* und *PH CH* weisen darauf hin, dass die in Artikel 9 verwendeten Begriffe und Definitionen unpräzise seien. Zudem fordern sie einen zusätzlichen Buchstaben mit folgendem Text: „Daten im elektronischen Patientendossier einen, von den Gesundheitsfachpersonen erfassten Primärdaten unabhängigen Lebenszyklus haben". Die *ISSS* fordert bezugnehmend auf Absatz 1 Buchstabe c einen zusätzlichen Buchstaben d. Es würden keine Anforderungen an die ordnungsgemässe Datenhaltung bzw. ein Nachweis der Integrität gefordert, was mitaufzunehmen sei, da andere Gesetze konkrete Vorgaben machen würden (z.B. Geschäftsbücherverordnung (GeBüV), Art. 3). Konkret seien Daten des elektronischen Patientendossiers so aufzubewahren, dass ein Nachweis der Integrität möglich sei, d.h. eine nachträgliche Änderung der Daten liesse sich feststellen (z.B. durch Benutzer, eine technische Fehlfunktion oder Missbrauch / Cyberangriffe).

Absatz 1 Buchstabe a: Die *GDK* sowie 18 Kantone[32] sind der Meinung, dass die standardmässige Löschung medizinischer Daten nach 10 Jahren weder im Interesse der Patientinnen / Patienten sei und auch aus Sicht der medizinischen Behandlungsabläufe keinen Sinn mache. Die *GDK* und 8 Kantone[33] sprechen sich dafür aus, dass die Patientin / der Patient die Möglichkeit erhalten solle, die Dauer der Aufbewahrung der Daten auf eine längere Dauer als 10 Jahre zu befristen. Der Kanton *ZH* und der *ZAD* wünschen eine Überarbeitung der Bestimmungen über die Dauer der Aufbewahrung der Daten. Es sei eine wesentlich längere allgemeine Aufbewahrungsfrist (z.B. lebenslänglich) festzusetzen. 8 Stellungnehmende[34] weisen darauf hin, dass der Beginn der Laufzeit der 10 Jahre zu klären sei. Neben der Frage nach dem Laufzeitbeginn sei gemäss dem Kanton *ZG*, dem *KDSBSON*, dem *DSBAG* und *privatim* Buchstabe a auch betreffend der Informierung der Patientin / des Patienten vor der Datenlöschung zu ergänzen. Gemäss dem *HÄ CH* und der *ÄTG* müsse vor einer geplanten Löschung auch der behandelnde (Haus-)Arzt zeitgerecht informiert werden. Gemäss 6 Kantonen[35] sei zu beachten, dass mit dieser Regelung Artikel 40 Absatz 1 des Bundesgesetzes über Arzneimittel und Medizinprodukte (HMG), nach welchem Daten zur Verwendung von Blut oder Blutprodukte 30 Jahren zu archivieren seien, nicht eingehalten werde.

11 Stellungnehmende[36] fordern die Streichung von Buchstabe a. Der *VAKA* verweist darauf, dass auch

[32] AI, BL, GL, OW, UR, LU, SZ, BS, SH, ZH, ZG, TG, FR, GE, VS, VD, JU, NE
[33] BL, GL, OW, UR, LU, SZ, SH, TG
[34] AG, AR, TG, ZG, Post, KDSBSON, DSBAG, privatim
[35] FR, GE, VS, VD, JU, NE
[36] economiesuisse, Bleuer, Insel, K3, VZK, SBC, BS, NW, VAKA, SUVA, medshare

die dazugehörenden Erläuterungen sowie die anderen entsprechenden Nennungen mit einer fixierten Ablauffrist der Dokumente zu streichen seien. *Economiesuisse* schreibt dazu, dass die relevanten Daten bezüglich Gesundheit und Sicherheit ausnahmslos im elektronischen Patientendossier erfasst sein müssen. Die *Insel* weist darauf hin, dass die Maximalfrist von 10 Jahren nicht opportun sei und zudem von kantonalen Aufbewahrungsfristen abweiche. Die *BRH* bezieht sich ebenfalls auf die kantonalen Regelungen in dem sie, analog der bernischen Gesetzgebung, die Erhöhung der Zeitdauer auf 10 Jahre nach letzter Konsultation fordert. Die *K3* und der *VZK* machen darauf aufmerksam, dass diese Regelung auch im Widerspruch zur jener im Kanton Zürich stehe. Der Kanton *AG* schreibt, dass die Frist von 10 Jahren für behandlungsrelevante Daten im elektronischen Patientendossier (Sekundärsystem) kompatibel mit Vorgaben zur Aufbewahrung der Krankengeschichte im Primärsystem sei, da nach aargauischem Gesundheitsgesetz die Krankengeschichte ebenfalls zehn Jahre aufbewahrt werden müsse. Die *Post* fordert schliesslich, dass die Patientin / der Patient über die Löschung entscheiden dürfe und sich dies nicht nach den Aufbewahrungsfristen des Kantons richten solle. Der Kanton *NW* macht geltend, dass die separate Datenhaltung auch aus Sicht des Datenschutzes nichts bringe, da die besonders schützenswerten Daten ohnehin bereits im KIS von grossen Leistungserbringern abgelegt seien. Die getrennte Datenhaltung sei durch sicherheitstechnische Vorgaben zu ersetzen. Die *K3* und der *VZK* erachten die Vernichtung der Daten im elektronischen Patientendossier nach 10 Jahren als nicht sinnvoll, da die elektronischen Patientendossiers im besten Fall ein Leben lang funktionieren sollen. Ähnlich sind auch *H+*, der *SBK*, der *SVBG* und die *SWOR* der Ansicht, dass ein Dossier während der Lebenszeit der Bürgerinnen und Bürger verfügbar sein solle, damit es auf Wunsch wieder reaktiviert werden könne. Als Alternative zur Streichung schlagen sie vor, dass eine Vernichtung der Daten nach vorgängiger Ankündigung nur erfolge, wenn 10 Jahre auf diese elektronischen Patientendossiers kein Zugriff erfolge, bei Aufhebung oder bei Tod. Die Regelung solle so gestaltet werden, wie sie in Artikel 20 für das gesamte elektronische Patientendossier vorgesehen sei. Die *STSAG* plädiert dafür, dass das Löschen und Aufheben von Daten in alleiniger Obhut der Patientinnen / Patienten liegen solle, oder nach 10-jähriger Inaktivität automatisch gelöscht werden solle. *Santésuisse* weist auf die Gefahr hin, dass aufgrund der Befristung ein potentieller Datenverlust mit u.U. negativen medizinischen Konsequenzen entstehen könne. Das *KSOW* verweist darauf, dass von Gesundheitsfachpersonen erfasste Daten nach 10 Jahren zu löschen seien und fragt, ob auch andere Daten erfasst sein können. Gesundheitsdaten die längeren Fristen unterliegen dürften nicht einfach nach 10 Jahren gelöscht werden (z.B. chronische Erkrankungen). Die Aufbewahrungsfrist von relevanten Daten müsse im spezifischen Fall festgelegt werden.

6 Kantone[37] machen folgenden Formulierungsvorschlag für Buchstabe a: „[…] sont conservées jusqu'à la suppression du dossier électronique du patient, même si ceux-ci sont supprimés dans le système primaire après le délai légal de conservation des données spécifiés dans les lois cantonales". Der *HÄ CH* und die *ÄTG* sprechen sich für die Anhebung der Zeitlimite von 10 Jahren auf mindestens 15 oder mehr Jahre aus. Die *IG eHealth* und *PH CH* schlagen folgende Formulierung von Buchstabe a vor: „dass der Patient informiert wird, wenn von einer Gesundheitsfachperson im elektronischen Patientendossier erfasste Daten 10 Jahre nicht mehr abgerufen wurden". *PharmaSuisse* empfiehlt, alle Daten im elektronischen Patientendossier gleich zu behandeln und daher Buchstabe a folgendermassen zu ergänzen: „[…] vernichtet werden, sofern diese Möglichkeit nicht vom Patienten ausgeschlossen wurde". Konsequenterweise müsse diese Möglichkeit auch als Option in Artikel 3 aufgenommen werden: „i. Die automatische Vernichtung der im elektronischen Patientendossier erfassten Daten nach 10 Jahren (gemäss Art. 9, Abs. 1, Bst. a) auszuschliessen". *SCH* schlägt folgenden Zusatz vor: „[…] nach 10 Jahren vernichtet werden können". *Moeri* fordert seinerseits, dass keine Vernichtung nach 10 Jahren, sondern lediglich eine implizite Löschung nach Artikel 20 Absatz 1 erfolgt. Diese Frist solle nur für das Primärsystem gelten, für was auch der Kanton *BE* plädiert. Die *HL7*, *IHE*, die *BINT*, *Bleuer* sowie der Kanton *SG* schreiben, dass die Löschung dem Willen der Patientin / des Patienten zu überlassen sei. Gemäss dem Paradigma der abschliessenden Datenhoheit sei eine automatische Löschung durch die Betreiber nach 10 Jahren nicht zulässig. Nach der Meinung des Kantons *SG* haben die Gemeinschaften sicherzustellen, dass die im elektronischen Patientendossier erfassten Daten nach einer durch die Patientin / den Patienten frei wählbaren Dauer gelöscht werden. Sie / Er könne festlegen, dass die Daten unbefristet /

[37] FR, GE, VS, VD, JU, NE

lebenslang gespeichert werden. Die *Post* schlägt die Möglichkeit einer manuellen Löschung von Dokumenten, welche nicht weiter relevant sind (durch Patientin / Patienten oder Hausarzt) vor. Alternativ könne auch eine permanente Speicherung mit optionalem konfigurierbarem Ablaufzeitraum in Betracht gezogen werden. *Physioswiss* weist darauf hin, dass wesentliche medizinische Daten solange zur Verfügung stehen müssten, bis die Patientin / der Patient diese zur Löschung freigibt. Im Rahmen der Eröffnung des elektronischen Patientendossiers könne der Patientin / dem Patienten die Möglichkeit gegeben werden, eine Aufbewahrungsfrist zu wählen. Die Aufbewahrung der Daten müsse zudem auch über die Existenz einer Gemeinschaft hinaus sichergestellt werden, was auch ein Anliegen der *FMH* ist. Der *LUKS* fordert, dass Dokumente ohne Widerspruch der Patientin / des Patienten bis über ihren / seinen Tod im elektronischen Patientendossier verbleiben sollen. Die *Tessaris* schreibt, dass die von den Gesundheitsfachpersonen im elektronischen Patientendossier erfassten Daten nach Ablauf der von der behandelnden Gesundheitsfachperson nach Absprache mit der Patientin / dem Patienten festgelegten Dauer vernichtet oder gegen Zugriffe dauernd gesperrt werden sollen. Die *FMH* ist der Ansicht, dass die Regelung gemäss Buchstabe a dem Sinn und Zweck des elektronischen Patientendossiers entgegenwirke und schlägt vor, dass die Patientin / der Patient vor einer allfälligen Datenlöschung zu kontaktieren sei. Eine Löschung dürfe erst erfolgen, wenn die Patientin / der Patient diese freigibt oder das Dossier aufhebt. Ähnlich fordert der *VGIch*, dass die Aufbewahrungspflicht erst mit der Aufhebung des Dossiers auf Wunsch der Patientin / des Patienten, oder mit deren / dessen Ableben, endet. Gemäss dem Kanton *TI* soll Buchstabe a dahingehend geändert werden, dass die erfassten Daten bis zur Aufhebung des elektronischen Patientendossiers aufbewahrt werden. Die *SGMI* schreibt, dass eine grundsätzliche Datenvernichtung nach 10 Jahren keinen Sinn mache und schlägt vor, dass eine Patientin / ein Patient beantragen solle, dass Daten nach einer minimalen Aufbewahrungsfrist (nach Kanton und Art unterschiedlich) gelöscht werden.

Absatz 1 Buchstabe b: Die *Tessaris* schreibt, dass Buchstabe b auf ihren Änderungsvorschlag zu Buchstabe a abgestimmt werden solle. Daten seien auch nach Ablauf der von der behandelnden Gesundheitsfachperson festgelegten Dauer verfügbar zu machen. *SCH* schlägt statt „vernichten" folgende Definition vor: „[…] Daten sind gemäss aktuellem Stand der Technik unwiderruflich zu löschen". *PharmaSuisse* empfiehlt einen zusätzlichen Buchstaben für Absatz 1 mit folgendem Wortlaut: „im Fall der Vernichtung von Daten im elektronischen Patientendossier gemäss Buchstabe a, muss die Patientin oder der Patient mindestens 3 Monate im Voraus informiert werden". Gemäss der *FMH* solle sichergestellt werden, dass die Daten der Patientinnen / Patienten wiederhergestellt werden können, anstatt diese vollständig zu löschen. So wären diese bei einem Widerruf einer Patientin / eines Patienten wieder vorhanden. Zudem dürfe sich die Löschung nur auf Daten in der Gemeinschaft und allfällige Links beziehen. Die *medshare* wünscht die Neuformulierung von Buchstabe b betreffend der noch zu treffenden Regulierung zum digitalen Nachlass. Effektiv würden Daten erst nach dem Tod gelöscht und das nur, wenn innerhalb der noch zu definierenden Frist keine Erben die Aufrechterhaltung des Dossiers wünschen. 7 Kantone[38] fordern die Streichung von Buchstabe b.

Absatz 1 Buchstabe c: Die *HL7*, *IHE* und die *SGMI* wünschen eine Präzisierung, was Ablagen sind, die ausschliesslich dafür vorgesehen sind. Falls eine physische Separierung gemeint sei, müsste das definiert sein. Es frage sich grundsätzlich, ob eine Verordnung auf der Ebene Server oder Storage Technologie angesiedelt sein solle. Physische Trennungen eines virtuellen Dossiers auf virtuellen Infrastrukturen sei ein Widerspruch in sich. Für die *IG eHealth* und *SCH* ist unklar, was mit dem Wort „ausschliesslich" gemeint sei, da es als doppelte Ablage interpretiert werden könne. Dies wäre nicht zielführend. Sie schlagen die Streichung des Wortes „ausschliesslich" aus dem Buchstaben c vor. Der *VGIch* fragt wiederum, wie sich „dafür vorgesehene Ablagen" definiere und was technisch begründete Ausnahmefälle (siehe Erläuterungen) seien. Es werde ein gewichtiger Nutzen von IHE-tauglichen Repositories bei den Spitälern eliminiert, welche eine direkte Registrierung von lokalen Dokumenten erlauben würde. Es solle explizit erlaubt sein, dass die Stammgemeinschaft ein zentrales sekundäres Repository mit den Kopien aus dem Primärsystem führt. Zudem sei eine abschliessende Liste technischer Ausnahmefälle zu erstellen und die direkte Registrierung von lokalen Dokumenten in den Repositories der

[38] FR, GE, VS, VD, JU, NE, TI

Leistungserbringer als alternative Lösung zu erlauben. Die *medshare* wünscht ebenfalls die Präzisierung, der „Ablagen", die ausschliesslich dafür vorgesehen seien.

Der *VAKA* gibt zu bedenken, dass mit dieser Einschränkung sinnvolle funktionale Prozessmöglichkeiten ausgehebelt und aufgrund Redundanzen enorme Mehrkosten verursacht würden. Zudem werde dem Grundsatz von dezentralen Datenhaltungen gemäss dem Grundmodell widersprochen. In diesem Kontext würden für alle Gemeinschaften und deren Geschäftsmodelle wichtige Aspekte und Nutzen aus der gerichteten Verwendung ausgeschlossen. Es wird die ersatzlose Streichung von Buchstabe c inkl. der dazugehörenden Vorgaben in der TOZ gefordert. Neben dem *VAKA* fordern 8 weitere Stellungnehmende[39] die Streichung von Buchstabe c. Die Kantone *ZG*, *NW*, *ZH*, *SZ* und der *ZAD* schreiben, dass die separate Datenhaltung auch aus Sicht des Datenschutzes nichts bringe, da die besonders schützenswerten Daten ohnehin bereits im Primärsystem der Leistungserbringer abgelegt seien. Die getrennte Datenhaltung sei durch sicherheitstechnische Vorgaben zu ersetzen, denen ein Primärsystem zu entsprechen habe, damit es auch als Ablage für das elektronische Patientendossier verwendet werden dürfe. Das *LUKS* weist darauf hin, dass Buchstabe c das System unnötig verteuere. Das elektronische Patientendossier sei immer als virtuelles Dossier mit dezentralen Repositories definiert worden. Für diese Repositories seien Anforderungen zu definieren. Das *KSSG* fordert eine Umformulierung, so dass eine logische Trennung der Dokumente des elektronischen Patientendossiers von anderen Dokumenten möglich ist. Die *K3* und der *VZK* machen geltend, dass Spitäler Krankengeschichten bereits elektronisch führen. Die gleichen Daten nochmals in einem weiteren Repository zu speichern führe zu unnötigen Doppelspurigkeiten. Es genüge, wenn die Zugangsschlüssel für die Daten in separaten Ablagen gespeichert werden, die Daten selbst jedoch aus den jeweiligen spitalinternen Dossiers gelesen werden. *Privatim* verweist auf ein Telefonat mit dem BAG, wonach sich aus dieser Regelung ergeben, dass Daten aus den Primärsystemen nur in den sich, in den Gemeinschaften befindenden Repositories abgespeichert werden dürfen und damit eine Speicherung von Daten aus dem Primärsystem direkt im elektronischen Patientendossier ausgeschlossen sei. Diese Regelung erscheine zu wenig klar. Da es sich dabei um einen zentralen Punkt handle, sollte sich dieser mit einer klareren Formulierung, ohne Beiziehung der Erläuterungen, direkt aus dem Erlass ergeben. Für *HIN* und die *BINT* ist die Bereitstellung von dedizierten Datenspeichern nur für das elektronische Patientendossier übertrieben. Eine jederzeit nachvollziehbare logische Trennung der Daten genüge. Buchstabe c sei dementsprechend folgendermassen anzupassen: „[…] elektronischen Patientendossier so in hierzu geeignete Ablagen zu speichern, dass diese jederzeit von anderen Daten getrennt werden können (logische Trennung)". Entsprechende Anpassungen in den Erläuterungen seien ebenfalls nötig. Ähnlich schreibt das *USB*, dass die Möglichkeit der logischen Trennung der Sekundärdaten des elektronischen Patientendossiers gemäss den Erläuterungen auch in der Verordnung explizit festzuhalten sei und Buchstabe c folglich angepasst werden solle: „[…] elektronischen Patientendossier physikalisch oder logisch ausgeschieden geführt werden sollen".

Absatz 2: Die *IG eHealth*, *PH CH* und die *Post* bemängeln die Formulierung: „Sie haben auf Verlangen der Patientin oder des Patienten" und fragen, auf wen sich das „Sie" beziehe. Folgende Formulierung von Absatz 2 sei gemäss der *IG eHealth* und *PH CH* zu bevorzugen: „Die Gemeinschaften haben auf […]". Der Kanton *AI* weist an dieser Stelle darauf hin, dass die Speicherung der Daten und die damit verbundenen administrativen Abläufe den Datenschutzvorschriften anzupassen seien. Der Kanton *BE* und die *STSAG* sind der Meinung, dass die selektive Vernichtung von Patientendaten im elektronischen Patientendossier gänzlich durch die Patientin / den Patienten erfolgen müsse und nicht den Gesundheitsfachpersonen zugemutet werden könne. Die Instrumente dazu seien vorhanden; die Patientin / der Patient könne neue Daten in die Vertraulichkeitsstufe „geheim" steuern und diese dort dann löschen bzw. anderen Stufen zuweisen. Sie schlagen folgende Formulierung von Absatz 2 vor: „Sie haben der Patientin oder dem Patienten zu ermöglichen, die Verfügbarkeit der Daten nach Absatz 1 auf 10 bzw. 20 Jahre einzuschränken". Gemäss der *GDK* sowie 8 Kantonen[40] müsse es gelingen, die Leistungserbringer an das elektronische Patientendossier anzubinden und nicht zu riskieren, sie mittels komplizierter Vorschriften von einer Verwendung abzuschrecken. Die Vorgaben für die Befüllung und Verwaltung

[39] K3, VZK, LUKS, FMH, ZG, NW, ZH, ZAD
[40] BL, GL, LZ, OW, UR, NW, SH, SZ

der Dossiers durch die Behandelnden müssen so ausgestaltet sein, dass sie mit den Behandlungsabläufen vereinbar seien.

Absatz 2 Buchstabe a: 6 Kantone[41] wünschen die Streichung von Buchstabe a, da dies die Gesundheitsfachpersonen sowie deren Primärsystem betreffe und nicht die Gemeinschaft. Die *Insel* schreibt, dass Buchstabe a gestrichen werden solle und die Verantwortung den Patientinnen / Patienten gegeben werden solle. Das *KSSG* und der *VGIch* haben grosse Bedenken, ob die Ressourcen für die Befragung der Patientinnen / Patienten bestehen, ob ein Dokument veröffentlich werden soll, oder nicht. Das *KSSG* verweist darauf, dass die Patientinnen / Patienten Dokumente selber als „geheim" klassifizieren können. Gemäss dem *VGIch* seien auch software-technische Funktionsanpassungen in den Primärsystemen kaum zu realisieren, um diese Manipulationen auszuführen. Beide Stellungnehmende verlangen die Streichung von Buchstabe a. Die *Post* fragt, welche Daten gemeint und was die Kriterien, um diese Daten festzustellen, seien. Die Regelung sei zu umfangreich und in der Masse nicht machbar. Alternativ könne die Patientin / der Patient alle Daten die von Gesundheitsfachpersonen ins elektronische Patientendossier übertragen werden als „geheim" einstufen. Ähnlich wie die *Post* wünscht auch die *medshare* eine Präzisierung des Begriffs „Daten", was auch für andere Nennungen im Verordnungswerk gelte. Die *IG eHealth* und *PH CH* schlagen folgende Änderung von Buchstabe a vor: „alle neuen Dokumente ab einem vom Patienten bestimmten Zeitpunkt mit der Vertraulichkeitsstufe „geheime Daten" oder „sensible Daten" in seinem elektronischen Patientendossier zu speichern".

Absatz 2 Buchstabe b: 18 Stellungnehmende[42] wiederholen ihre Kommentare von Absatz 1 Buchstabe a in Bezug auf Absatz 2 Buchstabe b. Die *IG eHealth* und *PH CH* weisen darauf hin, dass Buchstabe b aufgrund ihres Vorschlages zu Buchstabe a zu streichen sei. Das *KSSG* verlangt ebenfalls die Streichung von Buchstabe b. Die Patientin / der Patient könne seine Dokumente in seinem vom elektronischen Patientendossier zur Verfügung gestellten Speicher ablegen, wenn er die Aufbewahrungsfrist verlängern möchte. Die *Post* fragt, ob hier die Gemeinschaft oder die Gesundheitsfachperson gemeint sei und falls es die Gesundheitsfachperson wäre, wie das funktionieren solle. Falls nicht die Gemeinschaft gemeint sei, bedürfe es einer Klärung. Der Kanton *NW* schlägt vor, dass der Patientin / dem Patienten die Möglichkeit geboten werde, ihre / seine Daten bis auf Widerruf aufzubewahren. *Moeri* bezeichnet Buchstabe b als obsolet. Die *SUVA* kritisiert bezüglich der Buchstaben a und b insbesondere den vorgesehenen Mechanismus, der ein aktives Einschreiten der Patientin / des Patienten bedinge und verlangt die Streichung von den beiden Buchstaben.

Absatz 2 Buchstabe c: Die *K3*, der *VZK*, der *VGIch* sowie die *Insel* wiederholen ihre Stellungnahme von Buchstabe a und fordern dementsprechend die Streichung von Buchstabe c. Für den *VAKA* ist der Usecase nicht ersichtlich. Bei Beibehaltung der Stufe „geheim" gehe dies eigentlich mit einem gleichen Effekt einher, ohne wesentlichen Aufwand, womit Buchstabe c zu streichen sei. Die *IG eHealth* und die *PH CH* fragen, was der Unterschied zwischen „löschen" und „vernichten" sei. Ähnlich weist *SCH* darauf hin, dass die Bedeutung von „vernichten" unklar sei. Die *IEGH* und *PH CH* schlagen folgende, alternative Formulierung vor: „[…] aus dem elektronischen Patientendossier zu löschen". *SCH* macht folgenden Vorschlag: „[…] aus dem elektronischen Patientendossier unwiderruflich zu löschen". Die *SMCF* schreibt, dass eine solche Vernichtung nicht möglich sein sollte, sondern nur eine Deaktivierung denkbar sei.

Absatz 3: Der *LUKS* und die *SGMI* machen geltend, dass das EDI und das BAG hier weitreichende Kompetenzen hätten. Während das *LUKS* die Streichung der Delegation an das EDI und das BAG sowie die Aufnahme der wichtigsten Anforderungen in die Verordnung fordert, spricht sich die *SGMI* für die Schaffung einer verwaltungsunabhängigen Kontroll- resp. Rekursmöglichkeit aus. Der *SBK*, der *SVBG*, die *SWOR* und *Physioswiss* begrüssen die im Rahmen von Absatz 3 festgelegten, zentralen Rahmenbedingungen sehr. Die berücksichtigten Grundlagen entsprechen internationalen Standards, welche den elektronischen Datenaustausch sicher regeln würden. Der *SBK*, der *SVBG* und die *SWOR* schreiben zudem, dass der Aufbau eines Kompetenzzentrums im Bereich der Semantik erforderlich sei.

[41] FR, GE, VS, VD, JU, NE

[42] Insel, AI, AR, BL, GDK, GL, OW, UR, LU, SZ, SH, SG, TG, ZG, ZH, ZAD, FMH, Physioswiss

Nur so könne die Nutzung von Referenzterminologien sinnvoll angehangen werden (SNOMED CT). Der *SBK* und die *SWOR* verweisen an dieser Stelle auf ihre Stellungnahme zur EPDV-EDI Anhang 3: Metadaten. Die *Post* wünscht, dass der Begriff „Integrationsprofile" zuerst eingeführt wird und beantragt ein Glossar, welches die wichtigsten Begriffe enthält. Der *LUKS* und die *FMH* weisen darauf hin, dass die Protokollierung der Zugriffe für die Behandelnden haftungsrechtliche Relevanz habe. Sie müsse zwingend dem Nachweis dienen, welche Daten ein Behandelnder zum Zeitpunkt eines Zugriffs gesehen hat. Dies sei in den weiterführenden Bestimmungen zu berücksichtigen. Der *VGIch* macht geltend, dass in den Protokolldaten auch die Zugriffe von Administratoren oder von Kontaktstellen-Personen sein müssen.

Die *FMH* ist der Meinung, dass auf die Regelung technischer Details auf Verordnungsebene zu verzichten sei und verweist auf ihre Stellungnahme in den generellen Bemerkungen. Dementsprechend fordern sie die Streichung von Absatz 3 Buchstaben b – d.

Absatz 4: 6 Kantone[43] weisen darauf hin, dass hier ein Fehler bei der Übersetzung ins Französisch bestehe. Das EDI könne zwar auf eine Übersetzung der Dokumente in die Landesprache verzichten, wenn das Originaldokument in Englisch ist, jedoch nicht auf eine Übersetzung in die anderen offiziellen Landessprachen, wenn das Originaldokument bereits in einer offiziellen Landessprache verfasst sei. Absatz 4 sei folgendermassen anzupassen; […] à les faire traduire dans les langues officielles". Die *FMH* fordert, dass die Vorgaben obligatorisch entweder in die 3 Landessprachen oder in Englisch verfügbar sein müssen. *SBC* fordert die Streichung von Absatz 4.

Absatz 5: Der *LUKS* und die *SGMI* wiederholen ihre Stellungnahme zu Artikel 9 Absatz 3. Ähnlich schreibt die *FMH*, dass die Delegationskompetenz des BAG zu streichen und mit einer Regelung auf Ebene Bundesratsverordnung zu ersetzen sei. Ansonsten sei eine verwaltungsunabhängige Kontroll- resp. Rekursmöglichkeit zu schaffen. Der *KDSBSON*, der *DSBAG*, *privatim* sowie die Kantone *ZG* und *BE* weisen darauf hin, dass eine Kann-Vorschrift nicht zielführend sei. Es sollte eine regelmässige (Periodizität festlegen) Überprüfung des Stands der Technik stattfinden und bei Veränderungen, die zu einer Bedrohungslage führen könnten, entsprechende Anpassungen vorgenommen werden. Sie schlagen folgende Änderung von Absatz 5 vor: […] (BAG) überprüft die Vorgaben nach Absatz 3 regelmässig auf ihre Vereinbarkeit mit dem Stand der Technik und nimmt bei Abweichungen, die zu einer Bedrohungslage führen könnten, Anpassungen vor". Die *K3*, der *VZK* und der Kanton *ZH* würden bevorzugen, wenn nur das EDI die Bestimmungen der Verordnung oder ihrer Anhänge ändern könne. Die *K3* und der *VZK* schlagen daher folgende Änderung von Absatz 5 vor: „Das EDI kann die Vorgaben […]". *HIN* verweist darauf, dass die Integrationsprofile und Austauschformate bei Einführung nicht vollständig seien. Es sollte ein geregelter Change- und Versionierungsprozess eingeführt werden, welcher Anpassungen mit den Beteiligten und den Betreibern abstimme, so dass jederzeit die Interoperabilität und die Austauschbarkeit von Daten garantiert blieben. Es wird folgende Anpassung von Absatz 5 empfohlen: „Hierbei ist insbesondere eine Abstimmung mit den Betreibern, eine Versionierung und die Rückwärtskompatibilität sicherzustellen, so dass die Austauschbarkeit von Daten jederzeit gewährleistet ist".

Art. 10	Zugangsportal für Gesundheitsfachpersonen
Das EDI legt die Anforderungen an das Zugangsportal für Gesundheitsfachpersonen fest.	

Der *VAKA* weist darauf hin, dass mehrere Zugangsportale (solche für Patientinnen / Patienten) genannt werden. Er fordert eine genauere Deklaration bzw. Vereinigung der Portale oder mindestens die Aussage, dass es ein Portal mit zwei verschiedenen GUI / Loginmasken sein könne. Zudem fordert der *VAKA*, wie auch der Kanton *AG*, dass die Begriffe „Daten" und „Dokumente" in sämtlichen Verordnungen einheitlich verwendet werden. Der Kanton *AG* schreibt zudem, dass ihm Transparenz im Zugangsportal als sehr wichtig erscheine und der Download von Dokumenten ins Primärsystem zum Erfüllen der Dokumentationspflicht begrüsst werde. Die *Post* wünscht die Klärung, ob ein Zugangsportal für Gesundheitsfachpersonen zwingend sei und ob es ein dediziertes Zugangsportal für Gesundheitsfachpersonen und Patientinnen / Patienten brauche. Die *BFH* schlägt vor, bereits hier auf den Anhang (TOZ)

[43] FR, GE, VS, VD, JU, NE

zu verweisen, damit die Anforderungen gefunden werden. Der *HÄ CH* und die *ÄTG* sprechen sich dafür aus, dass bezüglich dem Zugangsportal für Gesundheitsfachpersonen die Übersichtlichkeit durch geeignete Darstellung und Filter immer an oberster Stelle stehen solle. Nur so sei rationelles Arbeiten im Alltag möglich. Aktualität und Qualität der Daten gingen vor Quantität. Die *IG eHealth* und *PH CH* erachten die vollumfängliche Delegation der Definition der Zugangsportale für Gesundheitsfachpersonen an das EDI an dieser Stelle für sehr umfassend. Minimale Anforderungen an das Zugangsportal seien zu definieren. Sie machen in ihrem Kommentar zu Artikel 10 zudem einen detaillierten Formulierungsvorschlag für Artikel 10. Die *K3* und der *VZK* machen geltend, dass für die Gesundheitsfachpersonen ersichtlich sein müsse, wenn sie nur einen eingeschränkten Zugriff besitzen und verweisen auf ihren Änderungsantrag zu Artikel 3 Buchstabe f.

SCH und *economiesuisse* stellen fest, dass in den Empfehlungen von eHealth Suisse sowie der Botschaft zum EDPG der Zugriff auf Patientendaten auch mittels eines externen Zugangsportals vorgesehen war. In den aktuellen Verordnungen sei die Zertifizierung eines externen Zugangsportals nun nicht mehr enthalten. Ein „leichtgewichtiger" Zugang zum EPDG fehle somit bspw. für eine Gemeinschaft, welche nicht als Stammgemeinschaft fungieren wolle. *Economiesuisse* bedauert dies und *SCH* schreibt, dass dies für die Entwicklung von eHealth in der Schweiz nicht förderlich sei und innovative Use Cases im Bereich mHealth, Patient Empowerment und allgemeine Innovationen im Gesundheitswesen gebremst würden. Die *SGMI* und *SBC* schreiben, dass externe Portale auch in der Form von Mobile Applikationen realisiert werden können und diese wiederum weitere innovative Dienstleistungen anbieten. Sie fänden es schade, wenn sich mHealth komplett neben eHealth entwickeln würde. Ähnlich wie *SCH* fügen sie an, dass externe Portale einen wesentlichen Beitrag zu Patient Empowerment beitragen werden und Innovation durch neue Dienstleistungen von Drittanbietern ermöglicht würde. *SBC* zeigt in seiner Stellungnahme zudem ein konkretes Beispiel eines Anwendungsfalles zu diesem Thema auf. Die *HL7*, *IHE*, *SBC*, die *SGMI* und *economiesuisse* sprechen sich ebenfalls dafür aus, dass der EPDG-Vertrauensraum nicht nur für Leistungserbringer der Gemeinschaft als geschlossenes System organisiert sein sollte, da zertifizierte, externe Portale durch Innovation einen Mehrwert für die Patientinnen und Patienten sowie die Anbieter von online-Diensten und schlussendlich auch für das schweizerische Gesundheitssystem, die Wirtschaft und den Innovationsplatz Schweiz bringen würden. In einem identischen Vorschlag wünschen 6 Stellungnehmende[44] einen neuen Artikel 10bis „Externe Zugangsportale". Analog dem Formulierungsvorschlag von der *IG eHealth* und *PH CH* für Artikel 10 wird aufgrund des grossen Textumfangs für den genauen Wortlaut auf die online verfügbaren Stellungnahmen verwiesen.

Art. 11 Datenschutz und Datensicherheit

[1] Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben. Dieses muss insbesondere folgende Elemente umfassen:

a. die Benennung eines oder einer Datenschutz- und Datensicherheitsverantwortlichen;

b. ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen;

c. ein Verzeichnis der Datenablagen;

d. ein Verzeichnis der angeschlossenen Primärsysteme;

e. die Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen ;

f. die Datenschutz- und Datensicherheitsanforderungen an das Personal und Dritte.

[2] Sie müssen die im Datenschutz- und Datensicherheitsmanagementsystem als sicherheitsrelevant eingestuften Vorfälle der Zertifizierungsstelle und dem BAG melden.

[3] Das EDI legt die Anforderungen in Bezug auf Datenschutz und Datensicherheit fest.

[4] Die Datenspeicher müssen sich in der Schweiz befinden und dem Schweizer Recht unterstehen.

6 Stellungnehmende[45] erachten es als zielführender, die Vorgaben in Ziffer 11, die in Bezug auf den

[44] HL7, IHE, SBC, SGMI, economiesuisse, SCH

[45] ZH, NW, ZG, ZAD, K3, VZK

Datenschutz und die Datensicherheit erfüllt sein müssen, generell-abstrakt zu nennen. Es sei den Gemeinschaften und Stammgemeinschaften sowie Leistungserbringern zu überlassen, wie sie diese Vorgaben einhielten. Artikel 11 sei dementsprechend vollständig zu überarbeiten. Die *Post* schlägt die Veröffentlichung einer Liste mit den Rollen, welche eine Gemeinschaft besetzen müsse, vor. Denkbar wäre diesbezüglich auch ein Kapitel in den Erläuterungen. Der *VAKA* und der Kanton *AG* schreiben, dass ein Datenschutz- und Datensicherheitsmanagementsystem aus datenschutzrechtlicher Sicht zu begrüssen sei, es führe aber zu Aufwand für die Gemeinschaften. Sie wünschen die Aufnahme von Hinweisen in den Erläuterungen, wie diese Aufwände zu verhindern seien, z.B. dass mehrere Gemeinschaften gemeinsam eine unabhängige Person als Datenschutzverantwortliche(n) mandatieren oder anstellen können. Des Weiteren bezeichnet der Kanton *AG* die Formulierung der Verschlüsselungsthematik als schwammig. Die Vorgabe zur Verschlüsselung dürfe nicht erst in der TOZ, sondern bereits in der EPDV verankert werden. Die *SMCF* schreibt, dass es angesichts dieser Anforderungen legitim scheine, die Anzahl Gemeinschaften auf 10 und nicht auf 20 bis 40 zu beschränken. Gemäss dem *VGIch* solle die Zuständigkeit bezüglich Datenschutz und Datensicherheit der Gemeinschaften am Leistungsübergabepunkt bzw. der Schnittstelle für Abfragen und Dokumenten-Einstellung der angeschlossenen Institution enden. Zur Regelung sei ein zusätzlicher Absatz in Artikel 11 aufzunehmen. Zusätzlich weist der *VGIch* darauf hin, dass Vorgaben und Ausführungen in der TOZ nicht in die Primärsysteme eingreifen dürfen und falls doch, höchstens Vorgaben im Sinne von allgemeinen Grundsätzen der Datensicherheit bestimmt werden sollten.

Absatz 1: Die *FMH* weist darauf hin, dass die Vorgaben des Datenschutzgesetzes anzuwenden seien und keine Überregulierung erfolgen solle. Die *SQS* macht betreffend der Formulierung von Absatz 1 folgenden Vorschlag: „Gemeinschaften müssen nach Art. 11 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz zertifiziert sein. Sie müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben. Dieses muss die Anforderungen des Art. 4 Abs. 2 Verordnung über die Datenschutzzertifizierung VDSZ vom 28. September 2007 und der Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 19. März 2014 des EDÖB erfüllen. Dieses muss[…]". Zusätzlich machen sie in ihrem Kommentar einen weiteren, alternativen Formulierungsvorschlag, welcher einen Verweis auf die international anerkannten ISO-Normen ISO 9001 und ISO/IEC beinhaltet. Die *OFAC* macht darauf aufmerksam, dass die Gemeinschaften als kantonale Organe den kantonalen Datenschutzbestimmungen unterliegen werden. Einige wichtige Konzepte des Datenschutzes, wie das Datenschutz- und Datensicherheitsmanagementsystem sowie der Zertifizierungsprozess würden in den meisten kantonalen Gesetzgebungen nicht existieren. Es sei zudem zu beachten, dass die Unterschiede zwischen den kantonalen Gesetzen sehr wichtig seien. Die Leitlinien für Mindestanforderungen des EDÖB, die für Datenschutz- und Datensicherheitsmanagementsysteme gelten, müssen für alle Arten von Organisationen gelten. *Economiesuisse*, *SBC*, die *HL7* und *IHE* fordern, dass Gemeinschaften das Datenschutz- und Datensicherheitsmanagementsystem delegieren können, da es sonst die Kosten unnötig in die Höhe treibe. Konkret fordern sie folgenden Zusatz bei Absatz 1: „[…] betreiben, oder durch Delegation betreiben lassen. Dieses muss […]".

Absatz 1 Buchstabe a: Das *LUKS* fordert die Streichung von Buchstabe a. Die Anforderungen, die Aufgaben und der Nutzen des Datenschutzverantwortlichen seien unklar. Dieser Ansicht sind auch die *GDK* und 6 Kantone[46]. Sie sowie 6 weitere Stellungnehmende[47] fordern, dass auf spezielle Datenschutz- und Sicherheitsverantwortliche zu verzichten sei. Der Kanton *AI* empfiehlt, auf die Einsetzung einer unabhängigen Stelle zu verzichten, wenn der zuständige Datenschutzbeauftragte Kapazitäten habe, diese Aufgabe zu übernehmen.

Absatz 1 Buchstaben b und c: Die *ISSS* macht für den Buchstaben b folgenden, präzisierten Formulierungsvorschlag: „b. Ein System zur proaktiven Erkennung von und zum Umgang mit Vorfällen im Bereich Angriffssicherheit und Betriebsausfallsicherheit" und der Buchstabe c solle künftig folgendermassen lauten: „c. ein Verzeichnis der Datenablagen, Berechtigungen und Prozesse zur Datensicherung

[46] BL, GL, LU, OW, UR, SZ
[47] ZAD, NW, ZH, ZG, K3, VZK

und sicheren Aufbewahrung".

Absatz 1 Buchstabe d: Der *KDSBSON* und der *DSBAG* weisen darauf hin, dass in der Ausarbeitung der Gesetzgebung zum elektronischen Patientendossier nie die Rede davon gewesen sei, dass die Primärsysteme direkt an das elektronische Patientendossier angeschlossen würden. Vielmehr sei ein entsprechender Anschluss der Sekundärsysteme vorgesehen gewesen, was auch dem Kanton *FR* auffiel. Sie wünschen die Prüfung, ob wirklich ein Anschluss der Primärsysteme stattfinden solle, was aus datenschutzrechtlicher Sicht problematisch und nicht empfehlenswert erscheine. Würde tatsächlich ein Anschluss der Primärsysteme angestrebt, müssten diese die datenschutz- und informationssicherheitsrechtlichen Vorgaben der Gesetzgebung zum elektronischen Patientendossier erfüllen. Die *privatim* verweisen auf ihre Ausführungen dazu unter den allgemeinen Bemerkungen. Die *SQS* macht darauf aufmerksam, dass das Datenschutzmanagementsystem nach VDSZ als auch das Managementsystem nach ISO 9001 und das Informationssicherheits-Managementsystem ISO/IEC 27001 jegliche Systeme und nicht nur angeschlossene Primärsysteme umfassen würden. Auf eine explizite Nennung als Anforderung könne folglich verzichtet werden, wenn eine dieser Zertifizierungsnormen als Zertifizierungsnorm für die Gemeinschaften und Stammgemeinschaften gewählt würde. Dementsprechend werde die Streichung von Buchstabe d empfohlen. Gemäss dem Kanton *BE* suggeriere die Formulierung, dass die Primärsysteme „direkt" an das elektronischen Patientendossier angeschlossen seien. Tatsächlich seien sie über die Dokumentenablage (synchronisierte Kopie) nur indirekt mit dem elektronischen Patientendossier verbunden. Folgende Formulierung sei dementsprechend geeigneter für Buchstabe d: „d. ein Verzeichnis der abgebildeten Primärsysteme". Die *FMH* fragt, was Buchstabe d bedeute und ob dies realistisch und zumutbar sei. Buchstabe d sei zu streichen resp. durch ein Verzeichnis der Sekundärablagen zu ersetzen. Ähnlich sehen 6 Kantone[48] den Verordnungstext von Buchstabe d ebenfalls als unklar an. Die Daten, welche im Verzeichnis enthalten sein müssen, seien zu präzisieren, bspw. im erläuternden Bericht. Es sei nicht möglich, eine Liste von Computern und verwendeter Software von tausenden Gesundheitsfachpersonen zur Verfügung zu stellen. Buchstabe d sei dementsprechend zu streichen. Der Kanton *NE* fügt an, dass zumindest Details zu den Daten, die das Verzeichnis der Primärsysteme enthalten solle, im Verordnungstext oder dem erläuternden Bericht, aufzunehmen seien. Die *ISSS* macht für den Buchstaben d folgenden, präzisierten Formulierungsvorschlag: „[…] Primärsysteme, welche direkten oder indirekten Zugang zu den Daten / Kommunikation haben oder erlangen können". *Lovis* wünscht die Klärung, ob das Verzeichnis der angeschlossenen Primärsysteme Organisationen oder Systeme beinhaltet.

Absatz 1 Buchstaben e und f: Für *CURAVIVA*, den *Insos* und den Kanton *TG* sei diese (Unter-) Delegationsnorm zu vage. Sie sollte den Inhalt oder zumindest die grundlegenden Elemente der Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen sowie für das Personal und Dritte angeben. Es gehe dabei um die Lesbarkeit des Gesetzes, die richtige Anwendung durch die Betroffenen Akteure und im Endeffekt um die Rechtssicherheit. Der *senesuisse* erachtet die Regelung in den Buchstaben e und f als ungenügend. Gegenüber den Gemeinschaften müsse klarer bestimmt sein, welche Anforderungen sie von den Gesundheitsbetrieben und Gesundheitsfachpersonen sowie dem Personal und Dritten verlangen müssen. Entweder müsse der Text der Verordnung ergänzt werden oder eine Vollzugshilfe mit geeignetem Inhalt vorformuliert werden.

Absatz 2: Die *HL7* und *IHE* sprechen sich für die Festlegung einer Frist zwischen Eintreten und Meldung von solchen Vorfällen aus. Ähnlich bittet die *medshare* diesbezüglich um die Bestimmung einer Periodizität. Die *Post* fragt, welche Anforderungen an die Notifikation gestellt werden und empfiehlt, dass diese Vorschrift an die neue EU-Datenschutzrichtlinie angepasst sein solle. Für die *SPO* ist nicht klar, ob diese Meldepflicht verbindlich festgehalten sei und ob als sicherheitsrelevant eingestufte Vorfälle definiert seien. Sie bittet um eine verständliche und klare Formulierung. Die *FRC* bittet ebenfalls um die Klärung der Modalitäten und insbesondere der Frist für die Meldungen von Vorfällen im System. Die Reaktion müsse möglichst unmittelbar erfolgen.

[48] GE, VS, VD, JU; FR, NE

Die *SQS* macht geltend, dass Zertifizierungsstellen ausschliesslich für die Zertifizierung nach Massgabe der Zertifizierungsvorschriften zuständig seien und jährlich die Stammgemeinschaften und Gemeinschaften nach Zertifizierungsverfahren auditieren würden. Ihnen komme keine Rolle im operativen Geschäft in der Zeit zwischen den Audits zu. Daher seien Vorfälle nach Absatz 2 lediglich ans BAG resp. nicht an Zertifizierungsstellen zu melden. Mittels Artikel 36 Absatz 1 Buchstabe c sowie Artikel 37 Absatz 3 Buchstabe a dieser Verordnung könne das BAG die Zertifizierungsstellen einbeziehen, falls aufgrund von Meldungen über wesentliche, sicherheitsrelevante Vorfälle mittels einer Überprüfung durch die Zertifizierungsstelle drohende Verletzungen des Datenschutzes und der Datensicherheit verhindert werden müssten. Die *OFAC* schreiben, dass der EDÖB zur Gewährleistung seiner Unabhängigkeit beim Bund angegliedert sei. Es sei normalerweise Sache des Bundes, die Schwere eines Vorfalles zu bewerten und über Massnahmen betreffend den involvierten Parteien zu entscheiden. Dies sei in diesem Falle für das EDI und BAG das gleiche.

Absatz 3: Gemäss der *SGMI* sei sicherzustellen, dass die Anforderungen in Bezug auf Datenschutz und Datensicherheit kongruent mit dem Datenschutzgesetz seien und nicht weiter gingen. Ähnlich schreibt das *LUKS*, dass keine Überregulierung erfolgen solle, sondern das Datenschutzgesetz auch hier gelte. Eine zusätzliche Regelung sei nicht nötig, womit Absatz 3 überarbeitet werden sollte. Die *ISSS* und die *Tessaris* schlagen folgenden Zusatz bezüglich Absatz 3 vor: „[…] Datenschutz und Datensicherheit und deren Anpassung an die Entwicklung der Bedrohungslage fest". Die *SQS* weist analog ihres Kommentars von Absatz 1 darauf hin, dass bei einer Wahl der Zertifizierung nach VDSZ, die Anforderungen in den „Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem" vom 19. März 2014 des EDÖB definiert seien. Dementsprechend müssten nur zusätzliche Erfordernisse festgehalten werden. Die *OFAC* sind der Meinung, dass die Anforderungen in Bezug auf den Datenschutz von einem Eidg. Departement, anstatt eines Dienstes des EDÖB, festgelegt werden sollten. Mit der Festlegung der Anforderungen komme auch die Kontrolle deren Einhaltung. Die Dienste des EDÖB seien in der Bundeskanzlei angesiedelt. Dadurch werde die Neutralität der Kontrollen sowie der Überwachung gewährleistet. Eine Überwachung, die durch das BAG durchgeführt wird, sei nicht neutral, insbesondere hinsichtlich den zentralen Forschungsdiensten, welchen unter der BAG-Verantwortung bleiben.

Absatz 4: Der *KDSBSON*, der *DSBAG*, die *privatim* sowie die Kantone *BE* und *FR* erachten diese Regelung aus datenschutzrechtlicher Sicht als zwingend, da es sich bei Gesundheitsdaten um besonders schützenswerte Personendaten handle und im Rahmen des elektronischen Patientendossiers auch die Gefahr der Entstehung von Persönlichkeitsprofilen bestehe. Es sei zusätzlich zu prüfen, ob nicht auch der Firmensitz und der Arbeitsplatz aller involvierten Mitarbeitenden zwingend in der Schweiz sein müssen. Ähnlich weist der Kanton *TG* darauf hin, dass eine Bearbeitung der Daten im Ausland zu vermeiden sei und der Absatz entsprechend ergänzt werden müsse. Die *ISSS* macht einen konkreten Formulierungsvorschlag: „Die Datenleitungen, Datenverbindungen, Datenübermittlung, Datenspeicherung und Datenverarbeitung müssen sich in der Schweiz befinden und dem Schweizer Recht unterstehen". *HIN* verstehe und unterstütze die Intention von Absatz 4. Sie fügt an, dass juristische Personen explizit erwähnt werden sollten und schlägt dementsprechend folgende Formulierung vor: „Leistungen zur Datenspeicherung müssen von juristischen Personen erbracht werden, die in der Schweiz domiziliert sind und Schweizer Recht unterstehen. Die Datenspeicher müssen […]".

Art. 12	Kontaktstelle für Gesundheitsfachpersonen
Die Gemeinschaften müssen für die Gesundheitsfachpersonen eine Kontaktstelle bezeichnen, die diese im Umgang mit dem elektronischen Patientendossier unterstützt.	

CURAVIVA, der *Insos* und der Kanton *AG* begrüssen die Einrichtung von Kontaktstellen für die Gesundheitsfachpersonen. Der *SBK*, die *SWOR* und *Physioswiss* erachten eine kompetente Unterstützung der Gesundheitsfachpersonen als entscheidenden Erfolgsfaktor für die erfolgreiche Realisierung des elektronischen Patientendossiers. Der *senesuisse* begrüsst die Schaffung solcher Anlaufstellen ebenfalls, weist aber darauf hin, dass deren Finanzierung längerfristig gesichert sein müsse, was mit den vorgesehenen Finanzhilfen nicht ausreichend gewährleistet sei. Der *HÄ CH* und die *ÄTG* machen geltend, dass Hotline-Angebote sehr schnell viel Geld und Zeit kosten können. Es müsse gerade in der

Anfangsphase für eine genügend hohe Kapazität gesorgt werden. Zudem müsse der Betrieb idealerweise kostenlos oder wenigstens kostenplafoniert sein. Diese Zusatzkosten gelte es im Tarif zu berücksichtigen und abzugelten. Sie betonen, dass Anpassungen von Primärsystemen, Schnittstellen, Zertifizierung, Hotlines etc. keine Businesscases sein dürfen. Die *BINT* fordert einen neuen Artikel anschliessend an Artikel 12 mit folgendem Text: „Die Gemeinschaften stellen sicher, dass der gemeinschaftsübergreifende Zugriff auf ihre Daten, bei Vorliegen der Patientenbewilligung, jederzeit und kostenlos möglich ist". Das *KSSG* kritisiert, dass die Ausprägung dieses Unterstützungsservices sehr vage sei. Einige Merkmale würden in der TOZ ausgeprägt, andere Merkmale – schwergewichtig organisatorische – seien gänzlich offen. Der Kanton *BS* weist darauf hin, dass den Gemeinschaften freigestellt sein müsse, ob sie eine oder mehrere Kontaktstellen für die Gesundheitsfachpersonen bzw. Patientinnen / Patienten führen. Sowohl in Artikel 12, wie auch in Artikel 19 sei dementsprechend zu ergänzen, dass mindestens eine Kontaktstelle bezeichnet werden müsse.

Die *SPO* gibt zu bedenken, ob gemäss der Verordnung klar sei, dass die in den Erläuterungen aufgeführten Vorgaben, wie z.B. „unterstehen einer der ärztlichen Schweigepflicht analogen Verpflichtung", auch eingehalten werden müssen.

2. Abschnitt: Stammgemeinschaften

Art. 14 Information der Patientin oder des Patienten

[1] Vor der Eröffnung eines elektronischen Patientendossiers muss die Stammgemeinschaft die Patientin oder den Patienten insbesondere über folgende Punkte informieren:

a. den Zweck des elektronischen Patientendossiers;

b. die Grundzüge der Datenbearbeitung;

c. die Folgen der Einwilligung und die Möglichkeit des Widerrufs;

d. die Erteilung von Zugriffsrechten.

[2] Sie muss der Patientin oder dem Patienten Datenschutz- und Datensicherheitsmassnahmen empfehlen.

Die *KKA*, die *KAeG SG*, der *BüAeV* und die *GAeSO* bemängeln, dass die Finanzierung der Aufklärung im Zusammenhang mit den Fragen der Patientinnen / Patienten nicht geregelt sei. Es sei davon auszugehen, dass die Stammgemeinschaften diese Kosten auf die ihr angeschlossenen Gesundheitsfachpersonen überwälzen werden, bspw. über Mitgliederbeiträge. Nach dem Verursacherprinzip müssten die Kosten im Zusammenhang mit der Aufklärung der Patientinnen / Patienten eigentlich auch von diesen getragen werden. Sie fordern die Aufnahme des folgenden, zusätzlichen Buchstaben in Absatz 1: „e. Bemessungsgrundlagen und Verwendung der zu bezahlenden Beiträge". Die *K3*, der *VZK* und der *VAKA* schreiben, dass die gegenüber den Patientinnen / Patienten zu kommunizierenden Informationen in Artikel 14, wie auch in der TOZ enorm weitreichend und sehr ausführlich beschrieben seien. Dies sei kaum der Sinn einer Information. Sie fordern eine Überarbeitung resp. eine pragmatischere, einfachere Festlegung. Die *K3* und der *VZK* fügen zudem an, dass die Empfehlung von Datenschutz- und Datensicherheitsmassnahmen für die Patientinnen / Patienten nicht zielführend sei. Sie würden die Implementation dieser Vorgaben als Standards im System bevorzugen. An dieser Stelle weist *FRC* darauf hin, dass die Patientin / der Patient auch darüber informiert sein müsse, ob ihr / sein Arzt, ihr Apotheker, etc. am elektronischen Patientendossier teilnehmen, oder eben nicht und was die damit verbundenen Konsequenzen sein können. *Santésuisse* ist der Meinung, dass der IDP resp. die Registrierungsstelle die Aufklärung machen. Ihrer Ansicht nach mache es Sinn, wenn die Patientin / der Patient beim Eröffnen des Dossiers resp. bei der Antragsstellung über die Folgen des elektronischen Patientendossiers informiert werden. Ansonsten müsste sie / er extra noch bei der Stammgemeinschaft vorbei gehen. Die *SPO* fordert 3 zusätzliche Absätze in Artikel 14: „Absatz 3: Sie stellt sicher, dass die in Art. 14.1 aufgeführten Informationen erfolgt sind und ist darüber beweispflichtig. Absatz 4: Sie informiert die Patientinnen und Patienten regelmässig und schriftlich über die erfolgten Bearbeitungen von Daten. Absatz 5: Sie stellen sicher, dass Änderungen im Bereich der Zugriffsrechte für Gesundheitsfachpersonen nach Art. 9 Abs. 3 und Art. 10 Abs. 2 Bst. b Ziff. 1 EPDG protokolliert werden".

Absatz 1: Aus Sicht des *SBK*, des *SVBG* und der *SWOR* sei die Kompetenz einer Stammgemeinschaft zur ausreichenden Information der Patientinnen / Patienten kritisch zu beurteilen. Die Stammgemeinschaft müsse sicherstellen, dass die Fachkompetenz für diese Patienteninformation gewährleistet werden könne. Das *KSSG* und die *SVP* wünschen eine genauere Definierung, wie die Informierung zu erfolgen habe. Das *KSSG* weist mittels eines Rechenbeispiels zudem darauf hin, dass eine direkte Aufklärung durch die Mitarbeitenden zu einem grossen Aufwand führen könne und fordert die Beschreibung der Form der Patientenaufklärung in den Ausführungsbestimmungen bzw. der TOZ. Gemäss 6 Kantonen[49] sei es auch wichtig, die Patientinnen / Patienten über die Konsequenzen eines Widerrufs zu informieren. Es gäbe einen Datenverlust und die Krankengeschichte wäre auch im Falle einer neuen Genehmigung nicht mehr vorhanden. Sie schlagen die Aufnahme eines zusätzlichen Buchstaben in Absatz 1 vor: „e. la possibilité de révoquer le dossier et les conséquences d'une révocation". Die *FRC* schlägt ihrerseits folgenden Zusatz für den Buchstaben c vor: „[…] consentement, ou d'un non consentement, et la possibilité […]". Die *SPO* bedauert, dass der Passus „aus einem Widerruf dürfen ihr oder ihm keine Nachteile erwachsen" im EPDG, 2. Abschnitt, Artikel 3.3 herausgestrichen worden sei. Es wird folgender Zusatz zu Absatz 1 Buchstabe c vorgeschlagen: „[…] des Widerrufs sowie die möglichen Folgen eines Widerrufs". *CURAVIVA*, der *Insos* und der Kanton *TG* weisen darauf hin, dass bei urteilsunfähigen Personen deren Stellvertretung informiert werden müsse und schlagen folgende Formulierung von Absatz 1 vor: „[…] oder den Patienten und gegebenenfalls ihre bzw. seine Stellvertretung insbesondere über die […]". *CURAVIVA* und der *Insos* schreiben zudem, dass die Patientinnen / Patienten, trotz ihrer Urteilsunfähigkeit, ebenfalls informiert werden müssten. Die *HL7*, *IHE* und die *Integic* machen einen ähnlichen Formulierungsvorschlag: „[…] oder den Patienten oder Stellvertreter/in insbesondere über folgende […]". Der *senesuisse* kritisiert ebenfalls, dass in diesen Regelungen Ausführungen zu Patientinnen / Patienten, welche nicht mehr urteilsfähig sind, fehlen würden. Da dies in der Praxis häufig vorkomme, seien entsprechende Ergänzungen vorzunehmen, welche sich auf Artikel 377 Buchstabe f ZGB abstützen. Die *privatim*, der *KDSBSON*, der *DSBAG* sowie die Kantone *BE* und *ZG* sind der Meinung, dass diese Regelung eine Verpflichtung der Stammgemeinschaft zur Aufklärung der Patientinnen / Patienten über mögliche informationssicherheitsrechtliche Risiken der Nutzung des elektronischen Patientendossiers vorsehen solle. Sie wünschen folgenden, zusätzlichen Buchstaben in Absatz 1: „e. die informationssicherheitsrechtlichen Risiken der Nutzung des elektronischen Patientendossiers". Die *Tessaris* macht folgenden, konkreten Formulierungsvorschlag für Absatz 1: „Die Stammgemeinschaften informieren die Öffentlichkeit, die Gesundheitsfachpersonen und Patienten in allgemeiner Weise über folgende Punkte betreffend Eröffnung, Betrieb und Aufhebung des elektronischen Patientendossiers". Zusätzlich schlägt sie bezüglich Buchstabe d folgenden Zusatz vor: „die Bedeutung der Festlegung der Vertraulichkeitsstufen sowie die Erteilung […]". Ähnlich macht die *FMH* geltend, dass auch über die Folgen einer Zugriffseinschränkung aufgeklärt werden solle.

Absatz 2: *CURAVIVA*, der *Insos* und der Kanton *TG* schlagen bezüglich der Informierung von Stellvertretungen urteilsunfähiger Personen auch einen Zusatz zu Absatz 2 vor: „[…] oder dem Patienten und gegebenenfalls ihrer bzw. seiner Stellvertretung Datenschutz- und Datensicherheitsmassnahmen empfehlen". Die *HL7*, *IHE*, die *Integic*, das *LUKS* und die *medshare* wünschen die Präzisierung der Empfehlungen und fragen, nach welchen Kriterien diese erfolgen sollen. Die *FMH* fordert die Streichung von Absatz 2. 7 Stellungnehmende[50] weisen darauf hin, dass die Datenschutz- und Datensicherheitsmassnahmen der Patientin / dem Patienten nicht empfohlen, sondern durch entsprechende technische Voreinstellungen (z.B. passwortgeschützte Zugänge, zwingende Verschlüsselungen usw.) vorgegeben werden sollten (Privacy by Default). Bei einer reinen Empfehlung würde die Verantwortung an die Patientin / den Patienten abgeschoben, was aufgrund der Art der bearbeiteten Daten nicht angemessen erscheine. Die *Tessaris* schlägt folgenden Verordnungstext für Absatz 2 vor: „Die Stammgemeinschaften machen die Gesundheitsfachpersonen sowie die Patientinnen / Patienten in allgemeiner Weise auf die Anforderungen aus dem Datenschutz und die Risiken für die im elektronischen Patientendossier gespeicherten Daten aufmerksam". Der *VGIch* weist darauf hin, dass die Information (Abs. 1) / Empfeh-

[49] GE, VS, VD, JU; FR, NE

[50] privatim, DSBAG, KDSBSON, BE, AG, ZG, ZAD

lung (Abs. 2) einer juristischen Beratung gleichkomme, welche in den Bereich der Tätigkeit mit Bewilligungsvorbehalten falle, eine entsprechende Ausbildung notwendig machen, und eine Haftung aus Beratung nach sich ziehen würde. Information und Empfehlung seien klar zu unterscheiden und die TOZ solle klarer formuliert werden.

Art. 15	Einwilligung
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 unterzeichnet sein.	

Der *SBK*, der *SVBG* und die *SWOR* fragen, was hier genau die Rolle der Stammgemeinschaft sei und ob diese bei Patientinnen / Patienten aktiv „Werbung" betreibe. Das *KSOW* und der Kanton *ZG* fragen, ob die Einwilligung und damit die Unterzeichnung auch elektronisch erfolgen könne. *Economiesuisse* bezeichnet die Möglichkeit zur elektronischen Unterschrift als sinnvoll und die Post schlägt ebenfalls vor, dass die elektronische Signatur als Einwilligung anerkannt werde. Gemäss *SCH* sei im Sinne des Ziels, eine grösstmögliche Digitalisierung zu erreichen, die qualifizierte elektronische Signatur gemäss Artikel 14 OR unmissverständlich zu akzeptieren. Darüber hinaus sollten auch andere Hilfsmittel zur eindeutigen Identifizierung von Personen zugelassen werden. Die Präzisierung solle zudem auf Stufe Verordnung klar ausformuliert werden. Es wird folgender Zusatz zu Artikel 15 vorgeschlagen: „ […] unterzeichnet sein. Zulässig ist auch die Nutzung anderer Hilfsmittel zur eindeutigen Bestimmung der Identität der Patientin oder des Patienten". Die *IG eHealth* und *PH CH* wünschen ebenfalls die Sicherstellung, dass die Einwilligung per elektronischer Unterschrift erfolgen könne und schlagen folgenden Wortlaut für Artikel 15 vor: „[…] Diese muss von der Patientin oder dem Patienten nach Artikel 14 Absatz 2bis des BG betreffend die Ergänzung des ZGB, 5. Teil: Obligationenrecht, unterzeichnet sein". Die *KKA*, die *KAeG SG*, der *BüAeV* und die *GAeSO* begrüssen, dass die Einwilligung von den Patientinnen / Patienten eigenhändig zu unterzeichnen sei bzw. eine der eigenhändigen Unterschrift gleichgestellte, elektronische Signatur vorliegen müsse. Die *Tessaris* schlägt vor, dass die Gesundheitsfachpersonen oder die Gemeinschaft von der Patientin / dem Patienten bei Beginn bzw. spätestens bei Beendigung der Behandlung die Einwilligung zur Führung des elektronischen Patientendossiers einzuholen habe. Diese müsse schriftlich abgefasst und unterzeichnet sein oder in einem von der behandelnden Gesundheitsfachperson vor Zeugen erstellten und unterzeichneten Protokoll festgehalten werden. Der *VAKA* bemängelt, dass die Definition „unterzeichnet" zu wenig klar sei. Er stelle sich diesbezüglich nicht handschriftlich im Sinne von Papier vor, sondern auch die Möglichkeit auf einem „Pad" zu unterschreiben. Es sei sicherzustellen, dass möglichst einfach rechtsgültig unterzeichnet werden könne, was auch die *Medgate*, die *K3* und der *VZK* fordern. Die *K3* und der *VZK* schreiben zudem, dass die Einwilligung von zu Hause aus, in einem Swisscom-Shop oder einer Poststelle möglich sein solle. Der Kanton *AG* weist darauf hin, dass die Schriftlichkeit und die eigenhändige Unterschrift aus Gründen der Beweissicherung geboten seien. Die elektronische Signatur würde den Vorgaben des OR entsprechen, wobei sie wohl in der Praxis immer noch nicht intensiv genutzt werde. Die *PKS* und die *SGMI* kritisieren, dass der Eröffnungsprozess eine ad-hoc Nutzung bei einem Leistungserbringer verhindere, da vorgängig bei der Stammgemeinschaft eine unterzeichnete Einwilligung vorliegen müsse. Die Eröffnung eines elektronischen Patientendossiers direkt beim Leistungserbringer sei zu ermöglichen und die Unterzeichnung müsse direkt vor Ort und ohne zusätzliche Infrastruktur möglich sein. *Santésuisse* schreibt, bezugnehmend auf ihren Kommentar zu Artikel 14, dass es auch hier Sinn mache, dass der IDP resp. deren Registrierungsstelle die Einwilligung bei der Registrierung einhole.

Die *Tessaris* schreibt, dass urteilsfähige Personen ihre Rechte am elektronischen Patientendossier selber oder durch einen von ihnen bezeichneten Vertreter ausüben könnten, für urteilsunfähige Personen sollen deren gesetzliche Vertreter handeln. Die *Post* bittet um eine Präzisierung, wie die Urteilsfähigkeit / Zurechenbarkeit der Patientinnen / Patienten geprüft werde und was passiere, wenn diese verloren gehe. Der *senesuisse* wiederholt an dieser Stelle seine Stellungnahme zu Artikel 14.

Gemäss der *KKA*, der *KAeG SG*, dem *BüAeV* und der *GAeSO* bestehe bei Vorliegen der Einwilligung die Vermutung, dass die Gesundheitsfachpersonen sämtliche gesundheitsrelevanten Daten ins elektronische Patientendossier stellen dürften, ausser die Patientin / der Patient hätte etwas anderes angeord-

net. Dies sei begrüssenswert. Aufgrund dieser Regelung sei allerdings damit zu rechnen, dass die Gesundheitsfachpersonen alle Daten in das elektronische Patientendossier stellen werden, so dass ihnen später kein Vorwurf gemacht werden könne, dass sie eine „wichtige" Information nicht abgelegt hätten. Um eine Datenschwemme zu verhindern sei den Gesundheitsfachpersonen ein grösstmögliches Ermessen in Bezug auf die Auswahl der behandlungsrelevanten Daten, welche in der Botschaft übrigens nicht ausreichend beschrieben seien, einzuräumen. Sie fordern einen zusätzlichen Artikel mit folgender Formulierung: „Ob Daten behandlungsrelevant und im elektronischen Patientendossier zu erfassen sind, liegt im Ermessen der Gesundheitsfachpersonen". Wie der *ZAD* bemängeln sie zudem, dass nach wie vor nicht geregelt sei, ob die Gesundheitsfachpersonen die von ihnen in das elektronische Patientendossier gestellten Daten anpassen oder löschen dürfen. Während der *ZAD* generell eine Regelung diesbezüglich verlangt, schreiben sie, dass für eine Berechtigung wohl direkt das EPDG angepasst werden müsse. Der Kanton *ZH* weist darauf hin, dass die Daten, welche im elektronischen Patientendossier zugänglich gemacht werden müssen, zu definieren seien. Zusätzlich sei zu klären, ob sich eine Ärztin / ein Arzt strafbar mache, wenn sie / er Daten nicht oder nicht vollständig übertrage.

Art. 16 Verwaltung

[1] Stammgemeinschaften müssen:

a. den Eintritt und den Austritt von Patientinnen und Patienten regeln;
b. die Patientin oder den Patienten identifizieren;
c. sicherstellen, dass Patientinnen und Patienten und deren Stellvertretung für den Zugriff auf das elektronische Patientendossier nur gültige Identifikationsmittel verwenden, die von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurden;
d. eine Patientenidentifikationsnummer nach den Vorgaben der Artikel 5 und 6 anfordern;
e. Prozesse zum Wechsel der Stammgemeinschaft vorsehen.

[2] Stammgemeinschaften müssen die Umsetzung der Artikel 2 Absätze 1–4 und Artikel 3 sicherstellen.

Der Kanton *AG* gibt zu bedenken, dass die genannten Verwaltungsaufgaben zwar erforderlich seien dürften, jedoch – wie auch der Wechsel der Stammgemeinschaft durch Patientinnen und Patienten - zu viel Aufwand für die Stammgemeinschaften führen würden. Die *medshare* macht folgenden Vorschlag zur Präzisierung von Absatz 1 Buchstabe a: „[…] die Eröffnung und den Widerruf des elektronischen Patientendossiers von Patientinnen und Patienten regeln". Für Buchstabe b wünscht sie folgenden Wortlaut: „die Patientin oder den Patienten authentifizieren und identifizieren". Die *Tessaris* schlägt folgenden Zusatz zu Absatz 1 Buchstabe b vor: „[…] identifizieren oder durch die antragstellende Gesundheitsfachperson identifizieren lassen". Der *VAKA*, die *K3* und der *VZK* weisen darauf hin, dass im Rahmen des Artikels nicht klar sei, ob die Verwendung der mTAN genügend sei und fordern die klare Nennung des Verfahrens mTAN und deren Zulassung als genügend (Folgeartikel und TOZ). Sollte die Patientin / der Patient ein für sie / ihn sichereres Verfahren wünschen, sei dies immer noch möglich. Die *Post* fragt, wie Artikel 16 für nicht in der Schweiz wohnhafte Personen auszulegen sei und bittet um Klärung. Im Zuge von Absatz 1 Buchstabe d machen die *IG eHealth* und *PH CH* geltend, dass aufgrund der aktuellen Regelung nur obligatorisch versicherten Personen nach Artikel 1 AHVG eine PID zugeteilt werden könne. Weitere Personen wie z.B. Grenzgänger könnten kein elektronisches Patientendossier haben und wären damit vom System ausgeschlossen, obwohl sie Anrecht auf Sozialleistungen aufgrund der bilateralen Verträge hätten. Die *IG eHealth* und *PH CH* weisen an dieser Stelle auf ihren Änderungsvorschlag von Artikel 5 Absatz 1 hin. Zudem sei ihnen Absatz 1 Buchstabe e zu offen formuliert. Sie schlagen deshalb folgenden Wortlaut vor: „[…] 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 elektronischen Patientendossier weiterhin in vergleichbarem Umfang erfolgen können. Das EDI legt den Umfang der Formate der zu transferierenden Daten fest". *Moeri* schreibt, dass Prozesse zum Wechsel der Stammgemeinschaft für Patientinnen / Patienten und deren Daten vorzusehen seien. Die Kantone *ZH*, *ZG* und *NW* sowie der *ZAD* weisen darauf hin, dass die Vorgaben direkter formuliert werden sollten. Die Stammgemeinschaften seien direkt zu verpflichten. Es sei vorzuschreiben, dass die Stammgemeinschaft gewechselt werden könne. Mit welchem Prozess die Stammgemeinschaft die Vorgabe umsetzt, sei ihr zu überlassen. Sie fordern eine vollständige Überarbeitung der Bestimmung und machen in ihren Stellungnahmen konkrete Formulierungsvorschläge, welche aufgrund deren Länge an dieser Stelle nicht aufgeführt werden.

Art. 17	Zugangsportal für Patientinnen und Patienten
Das EDI legt die Anforderungen an das Zugangsportal für Patientinnen und Patienten fest.	

CURAVIVA, der *Insos* und der Kanton *TG* kritisieren, dass die Formulierung dieser (Unter-) Delegationsnorm die Minimalanforderungen an Präzision und normative Dichte nicht erfülle. Artikel 17 solle nur schon hinsichtlich Transparenz und Lesbarkeit zumindest die grundlegenden Elemente der Anforderungen an das Zugangsprotal für Patientinnen / Patienten angeben. Die *FRC* schreibt, dass die Informierung der Patientinnen / Patienten im Rahmen der Verwendung des Zugangsportals schwierig werde. Sie schlägt vor, dass die Patientenorganisationen, die Integritätsschutz- sowie Beschwerdeorganisationen und die Verbraucherverbände zur Zusammenarbeit an den Informationsfunktionen eingeladen und im Sinne von Leistungsaufträgen bezahlt/vergütet werden. In diesem Kontext sollten sie ebenfalls ermuntert werden, miteinander für diese Aufgabe zusammenzuarbeiten. Die *SMCF* weist darauf hin, dass die Beurteilung dieser Zugangsmodalitäten für die Patientinnen/Patienten, basierend auf diesen Vorschriften schwierig sei. Diese Modalitäten werden aber eine wesentliche Rolle für den Einsatz des elektronischen Patientendossiers und für die Arbeitsbelastung der Gesundheitsfachpersonen in dieser Sache spielen.

Das *LUKS* schlägt die Aufnahme einer Regelung für die Zertifizierung von „externen" Patienten-Zugangsportalen, also solche keiner Stammgemeinschaft, vor. Auf sachlich nicht erforderliche Einschränkungen sei zu verzichten und innovative Lösungen / Geschäftsmodelle müssten möglich sein. 11 Stellungnehmende[51] befürchten, dass die Vorgaben des BAG mögliche Geschäftsmodelle zur Finanzierung des Betriebs des elektronischen Patientendossiers unverhältnismässig stark einschränken könnten. Das Ausführungsrecht, insbesondere die TOZ, sei so auszugestalten, dass die Entwicklung innovativer Lösungen und neuer Geschäftsmodelle möglich bleibe. Sie weisen ebenfalls darauf hin, dass auf sachlich nicht erforderliche Einschränkungen zu verzichten sei.

Der *SVBG*, *Physioswiss*, der *SBK* und die *SWOR* machen geltend, dass ein attraktives und hindernisfreies Zugangsportal eine wichtige Unterstützung für die Patientinnen / Patienten sein werde und somit einen Erfolgsfaktor darstelle. Der Kanton *AG* schreibt, dass klare Abgrenzungen auf dem Zugangsportal und Barrierefreiheit begrüsst werden. Der *VGIch* bringt ein, dass Grundzüge der Anforderung (z.B. barrierefreier Zugriff) in der Verordnung zu regeln seien und nicht erst in der EDI-Ausführung. Dem Legalitätsprinzip werde hier nicht entsprochen. Die *FMH* schreibt, dass gemäss Artikel 11 EPDG Zugangsportale zertifiziert sein müssten, unabhängig davon, ob sie Teil des Angebots einer Stammgemeinschaft oder einer normalen Gemeinschaft seien. Sie sind der Meinung, dass zumindest eine Regelung betreffend der Zertifizierbarkeit von Zugangsportalen von (Nicht-Stamm-)Gemeinschaft aufzunehmen sei.

Die *Post* ortet an dieser Stelle eine grosse „Machtkonzentration" beim EDI. Aus ihrer Sicht sollten bereits in den Verordnungen die Use Cases benannt werden, ohne dabei künftige Use Cases zu verhindern und fordert dementsprechend deren Definierung und Ergänzung. Für den *senesuisse* macht es den Anschein, als seien diese reinen Delegationsnormen an das EDI zu knapp ausgefallen. Zumindest die Grundzüge seien eindeutig in der Verordnung festzuhalten und demnächst zu veröffentlichen. Die *IG eHealth* und *PH CH* beschreiben diese vollumfängliche Delegation der Definition der Zugangsportale für Patientinnen / Patienten an das EDI als sehr unpassend. Die minimalen Anforderungen an das Zugangsportal seien zu definieren, damit ein einheitliches und interoperables Funktionieren des elektronischen Patientendossiers gewährleistet sei. Sie schlagen deshalb in ihren Stellungnahmen einen grundsätzlich neuen Artikel 17 vor, welcher aufgrund dessen Umfanges an dieser Stelle nicht aufgeführt wird.

Art. 18	Verfügbarkeit der von Patientinnen oder Patienten erfassten Daten
Das EDI legt die Anforderungen an den Umgang mit den von Patientinnen und Patienten über das Zugangsportal erfassten Daten fest.	

CURAVIVA, der *Insos*, der Kanton *TG*, der *senesuisse* und die *SMCF* wiederholen ihre Stellungnahmen

[51] GDK, BL, GL, OW, UR, LU, NW, ZH, SZ, ZG, ZAD

zu Artikel 17. Der *VAKA* verweist auf die Abhängigkeit zu TOZ 10.2 und schreibt, dass das Kosten-Nutzen-Verhältnis und insbesondere die Erweiterung ausserhalb eines Downloads bei einer vollumfänglichen Offline-Archivierung nicht gegeben seien. Ein Download der Dokumente sei bereits bei anderen Artikeln gegeben. Ein Import ausserhalb des reinen Patientendokumentes sei nicht möglich resp. sinnvoll. Der Kanton *AG* schreibt, dass eine klare abgegrenzte Ablage patienteneigener Daten begrüsst werde. Der Export patienteneigener Daten erscheine als zulässig und sinnvoll.

Art. 19 Kontaktstelle für Patientinnen und Patienten

Stammgemeinschaften müssen für die Patientinnen und Patienten eine Kontaktstelle bezeichnen, die sie im Umgang mit dem elektronischen Patientendossier unterstützt.

Der *senesuisse*, der Kanton *BS*, *CURAVIVA* und der *Insos* wiederholen ihre Stellungnahmen von Artikel 12, jedoch in Bezug auf Patientinnen / Patienten anstatt Gesundheitsfachpersonen. Die *SMCF* wiederholt ihren Kommentar von Artikel 17 und 18. Der *SBK*, der *SVBG*, die *SWOR* und *Physioswiss* erachten die Unterstützung der Patientinnen / Patienten in der Nutzung als entscheidender Erfolgsfaktor für die Realisierung des elektronischen Patientendossiers. Der *SBK*, der *SVBG* und die *SWOR* schlagen zudem eine Prüfung für Unterstützung seitens der nationalen Behörden vor. Für den Kanton *AG* erscheint ein Service-Desk für Patientinnen / Patienten als notwendig. Beratung und Beschwerden sowie Ombutsaufgaben würden jedoch zu einem nicht unerheblichen Mehraufwand führen. Gemäss der *FRC* sei es wichtig, dass die Stammgemeinschaften eine Kontaktstelle zur Unterstützung der Patientinnen / Patienten in der Nutzung des elektronischen Patientendossiers bezeichnen. Auch hier erscheine es wichtig, dass die Patientinnen / Patienten über mehrere Service- und Supportinformationen verfügen. Diese zusätzlichen Informationen sollen auch von ausserhalb der Gemeinschaft stammen, um Interessenskonflikte zu vermeiden und die Unabhängigkeit zu garantieren. Eine sehr gute Koordination des Informationsflusses sei das Ziel.

Das *KSSG* fragt, welche Anforderungen betreffend Reaktionszeiten gestellt werden. Für den Aufbau eines Service-Desk müssten in einer Stammgemeinschaft ca. 2-3 Mitarbeitende eingesetzt werden, um die Wartezeiten kurz zu halten. Falls die Reaktionszeiten Bestandteil der Zertifizierung sind, sei der Artikel in den TOZ auszuführen. Der *VGIch* schreibt, dass dieselben Vorgaben zu Protokollierung wie bei den Gesundheitsfachpersonen gelten würden. Hier seien Lücken in der Verordnung bzw. Undeutlichkeiten in den Erläuterungen feststellbar. Es gelte die Durchgängigkeit sicherzustellen. Zugriffe seien von allen zu protokollieren. Die *H+* machen geltend, dass es für eine praxistaugliche Umsetzung in Spitälern unumgänglich sei, dass fachverantwortliche Personen für das elektronische Patientendossier als Kontaktstelle für Patientinnen / Patienten bereitgestellt werden können. Der Ansatz, dass jede Gesundheitsfachperson diese Aufgabe erfüllen soll, sei nicht realistisch. Die Aufgabenspezialisierung bringe zudem einen fortwährenden Schulungsaufwand mit sich. Im Rahmen der „Datenlieferung für die Evaluation“ solle geprüft werden, wie dieser Mehraufwand analysiert und quantifiziert werden könne.

Art. 20 Aufhebung des elektronischen Patientendossiers

[1] Ein elektronisches Patientendossier wird von der Stammgemeinschaft aufgehoben, wenn:

a. die Patientin oder der Patient die Einwilligung zu dessen Führung widerruft;
b. während 10 Jahren niemand darauf zugreift; oder
c. die Patientin oder der Patient verstorben ist.

[2] Dazu muss die Stammgemeinschaft sämtliche Zugriffsrechte auf das entsprechende Patientendossier entziehen und:

a. im Fall der Aufhebung:
   1. alle Gemeinschaften sowie die ZAS innert angemessener Frist über die Aufhebung informieren,
   2. die Widerrufserklärung während 10 Jahren aufbewahren;
b. im Fall der Nichtnutzung nach Absatz 1 Buchstabe b die Patientin oder den Patienten 3 Monate vor der Aufhebung informieren.

Der *VAKA* verweist auf die Abhängigkeit zu TOZ 12.14.1 und schreibt, dass ein formloser Widerruf bzw.

Austreten nicht konform mit der Aufbewahrungspflicht (10 Jahre) sei. Der formlose Widerruf sei anzupassen auf Zitat: „nicht ganz formlos". 6 Kantone[52] schreiben, dass nicht aufgrund der Wirtschaftlichkeit elektronische Patientendossiers gelöscht werden sollten. Mit Blick darauf, was sonst alles kosten werde, sollte nicht am falschen Ort gespart werden. Sie fügen an, dass diese Fristen für die Erhaltung der Daten und des elektronischen Patientendossiers nicht der Notwendigkeit des elektronischen Patientendossiers entsprechen würden. Das elektronische Patientendossier gehöre der Patientin / dem Patienten ihr / sein Leben lang. Es enthält seine medizinischen Daten, welche für künftige medizinische Behandlungen notwendig sein können. *HIN* macht darauf aufmerksam, dass eine Löschung nach 10 Jahren ohne Zugriff im Hinblick auf die immer früher ermittelbaren Risikofaktoren oder medizinischen Informationen zur Patientin / zum Patienten nicht sinnvoll erscheine. Der *KKA*, die *KAeG SG*, der *BüAeV* und die *GAeSO* stellen fest, dass gemäss Artikel 20 die Daten (nach Art. 9, Abs. 1, Bst. b) zu löschen, die Protokolldaten jedoch 10 Jahre aufzubewahren seien. Gemäss Ziffer 2.10.2 TOZ enthielten die Protokolldaten keine medizinische Daten. Sie fragen, wie im Nachhinein über die Protokolldaten bestimmt werden könne, wer wann welche Daten abgerufen habe und ob die Daten, welche bei einem Widerruf zu löschen wären, nicht in einem separaten Archivbereich ohne Zugriff der Gesundheitsfachpersonen, aufbewahrt werden müssten. Die *K3* und der *VZK* schlagen vor, dass die Aufhebung des elektronischen Patientendossiers nicht unmittelbar, sondern erst nach einer bestimmten Frist erfolgen solle. Dies erlaube den Berechtigten bei Bedarf, z.B. für genetische Abklärungen, Daten zu sichern. Die *privatim* fordern an dieser Stelle die ausdrückliche Festhaltung, dass alle am elektronischen Patientendossier beteiligten Parteien, die im Zusammenhang mit dem elektronischen Patientendossier anfallenden Personendaten lediglich zur Erfüllung der ihnen durch das EPDG oder einen damit verbundenen Erlass übertragenen Aufgaben bearbeiten dürfen. Dies lasse sich zwar aus Artikel 4 Absatz 3 Datenschutzgesetz (DSG) ableiten, aufgrund der Art der im Zusammenhang mit dem elektronischen Patientendossier anfallenden Personendaten erscheine die Aufnahme einer Regelung jedoch als angemessen. Konkret schlagen sie folgende Formulierung vor: „1. Alle mit dem Aufbau, dem Betrieb und der Nutzung des elektronischen Patientendossiers betrauten Personen oder Institutionen dürfen die in dessen Zusammenhang anfallenden Personendaten ausschliesslich zum Zweck der ihnen durch das EPDG samt den dazugehörenden Ausführungserlassen übertragenen Aufgaben oder gestützt auf eine andere, hinreichend bestimmte gesetzliche Grundlage bearbeiten. 2. Eine Weitergabe von Personendaten zu Werbezwecken ist in jedem Fall untersagt". Gemäss dem Kanton *AG* seien die Vorgaben zu Widerruf, Löschung und der Aufbewahrungsfrist von 10 Jahren plausibel und auch die Aufbewahrungsfrist von 10 Jahren beweisrechtlich sinnvoll. Wichtig sei die vorgeschriebene Vorinformation der Patientinnen / Patienten 3 Monate vor der Löschung. *Lovis* ist der Ansicht, dass das elektronische Patientendossier nie gelöscht werden dürfe.

Absatz 1: Gemäss der *IG eHealth*, *PH CH* und *economiesuisse* könne die aktuelle Formulierung zur Löschung eines elektronischen Patientendossiers dazu führen, dass medizinische Daten der Patientin / des Patienten, ohne diesen zu benachrichtigen, automatisch unwiderruflich gelöscht werden. Da die Daten der Primärsysteme je nach kantonaler Regelung ebenfalls gelöscht werden müssten, könne dies zu einem ungewollten Datenverlust führen. Sie schlagen folgenden, neuen Buchstaben am Anfang des Absatzes vor: „a. nach unbeantwortetem Verstreichen einer Frist von 90 Tagen auf schriftliche Aufhebungsmitteilung an den Patienten, seine Vertreter und seinen Arzt des Vertrauens (Hausarzt)". Buchstabe c soll zudem folgendermassen lauten: „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." Die Buchstaben a – c würden neu zu Buchstaben b – d nummeriert. Die *STSAG* schlägt vor den Teil „kann von der Stammgemeinschaft aufgehoben werden" abzuändern. Die Stammgemeinschaft habe u.U. gar nicht Kenntnis von einem Todesfall, da die Meldepflicht nicht geregelt sei. Sie spricht sich dafür aus, dass das Löschen von Dokumenten und Aufheben des Dossiers (ausser im Todesfall) nur durch die Patientin / den Patienten möglich sein solle. Als Alternative könnten alle Dokumente immer gelöscht werden, wenn sie vor mehr als 10 Jahren ins elektronische Patientendossier gestellt wurden (in Primärsystem immer noch vorhanden und ggf. nachträglich wieder in Repository aufnehmbar, minimaler Administrationsaufwand). Gemäss der *SUVA* mache eine Aufhebung nur dann Sinn, wenn die Patientin / der Patient die Einwilligung

[52] GE, VS, VD, JU, FR, NE

zu dessen Führung widerrufe.

Absatz 1 Buchstabe a: Die *Tessaris* ist der Meinung, dass an den Widerruf grundsätzlich die gleichen Anforderungen wie an die Einwilligung zur Führung des elektronischen Patientendossiers gestellt werden sollten. Die Widerrufserklärung sollte im Übrigen geeignet sein, um die Anforderungen von Absatz 2 Buchstabe a Ziffer 2 zu erfüllen. Die *Tessaris* schlägt folgende Formulierung für Buchstabe a vor: „[…] dessen Führung durch unterschriftlich oder durch eine an die behandelnde Gesundheitsfachperson abgegebene und von dieser protokollierte und unterzeichnete Erklärung widerruft".

Absatz 1 Buchstabe b: Das *LUKS* schreibt, dass die Aufhebung des elektronischen Patientendossiers nach 10 Jahren ohne Zugriff nicht im Sinne einer lebenslangen Patientenakte sei und dem Nutzen des elektronischen Patientendossiers widerspreche. Gemäss der *FMH* sei dies nicht im Interesse der Patientinnen / Patienten und auch nicht im Sinne des Gesetzeszweckes. Für die *SGMI* macht eine generelle Löschung bei Nicht-Zugriff keinen Sinn und die Insel betrachtet die Frist von 10 Jahren als nicht angemessen. Die *Insel* fügt an, dass die Möglichkeit bestehe, Daten jederzeit löschen zu lassen (Art. 20, Abs. 1, Bst. a) und aus Gründen der Verständlichkeit zudem die Folgen der Aufhebung, d.h. die Löschung sämtlicher Daten, ausdrücklich in Absatz 2 Buchstabe a Ziffer 3 erwähnt werden. Die Frist solle auf 20 Jahre erhöht werden oder noch besser wäre es, im Default komplett auf eine Frist zu verzichten.

Der *HÄ CH* und die *ÄTG* machen geltend, dass diese Regelung nur nach vorgängiger Einverständniserklärung der Patientin / des Patienten und frühzeitiger Information des behandelnden Arztes gelte und verweisen auf den Kommentar zu Artikel 9 Absatz 1. Das gelte zudem auch für Absatz 2 Buchstabe b. Für die *ASPS* und den *Spitex* mache es mit dieser Zeitbegrenzung für gesunde Menschen wenig Sinn, ein elektronisches Patientendossier zu eröffnen. Menschen, die ein akutes Geschehen hatten und danach 10 Jahre gesund sind, würden ihre Registration verlieren. Eine zeitliche Beschränkung sei wegzulassen resp. beide Absätze zu streichen. Das *KSOW* weist darauf hin, dass zwischen einer Erfassung und einem nächsten Fall 10 Jahre verstreichen können. Die Daten dürften daher nicht automatisch gelöscht werden. Das Einverständnis der Patientin / des Patienten müsse zudem vorliegen. Der *SBK*, der *SVBG* und die *SWOR* sprechen sich für eine automatische Erneuerung des elektronischen Patientendossiers aus, solange keine anderen Anweisungen seitens der Patientin / des Patienten vorliegen. *Bleuer* schreibt, dass ohne Anordnung der Patientin / des Patienten Daten wohl mindestens 10 Jahre über den nachgewiesenen Tod hinaus aufbewahrt werden. Die *SMCF* weist darauf hin, dass lediglich eine Deaktivierung des elektronischen Patientendossiers möglich sein sollte und nicht eine automatische Löschung. Es sollen zudem die üblichen Fristen vor jeder Vernichtung von medizinischen Daten angewendet werden. Insgesamt sprechen sich 13 Stellungnehmende[53] für die Streichung von Buchstabe b aus, *Moeri* bezeichnet seinerseits den Buchstaben b als obsolet.

Absatz 1 Buchstabe c: 7 Stellungnehmende[54] weisen darauf hin, dass unklar sei, wie die Stammgemeinschaft vom Tod der Patientin / des Patienten erfahre. Allenfalls sei zu prüfen, inwiefern eine Meldepflicht durch die ZAS zielführend wäre. Sie fordern, dass dies geprüft werde und der Buchstabe c sowie der Artikel 9 Absatz 1 Buchstabe b je nach Resultat angepasst werden. Die *privatim*, der *DSBAG* und die Kantone *AG* und *BE* wünschen zudem die Prüfung, inwiefern eine Übergangsfrist von mehreren Jahren nach dem Tod einer Patientin / eines Patienten sinnvoll erscheine. Es könne für die Angehörigen aus mehreren Gründen notwendig sei, Zugriff auf das elektronische Patientendossier zu erhalten. Die *SGMI* weist ebenfalls darauf hin, dass u.U. noch auf das elektronische Patientendossier einer verstorbenen Person zugegriffen werden müsse und fordert, dass Buchstabe c mit einer angemessenen Frist versehen werde. Das *LUKS* bringt dieselbe Forderung vor und schlägt eine Frist von z.B. 3 Monaten vor. Die Möglichkeit, Dokumente nach dem Tod Angehörigen zu geben, sei zudem zu definieren. Das *KSSG* gibt zu bedenken, dass der Tod einer Patientin / eines Patienten einem Leistungserbringer nicht aktiv mitgeteilt werde. Es solle präzisiert werden, wann die Verpflichtung zur Aufhebung des Dossiers beginne und daher sei folgender Zusatz bei Buchstabe c zu ergänzen: „Bei Erlangung der Kenntnis, dass die Patientin […]". Die *Post* schreibt, dass zu klären sei, wie die Stammgemeinschaften den Tod

[53] LUKS, SGMI, FMH, ASPS, Spitex, GE, VS, JU, VD, NE, FR, Bleuer, SUVA

[54] privatim, DSBAG, KDSBSON, BE, SZ, ZG, AG

feststellen sollen. Ähnlich fordern der Kanton *ZH* und der *ZAD* die Klärung, wie die Stammgemeinschaften davon erfahren, dass Patientinnen / Patienten verstorben seien und weisen darauf hin, dass das elektronische Patientendossier nach dem Tod einer Patientin / eines Patienten nicht an Personen, die sie / er nicht ausdrücklich als Stellvertreter bezeichnet habe, zugänglich gemacht werden dürfe, was auch für Angehörige gelte. Die *K3* und der *VZK* bringen ebenfalls vor, dass die Gesundheitseinrichtungen und Gesundheitsfachpersonen nicht immer erfahren, wenn eine Patientin / ein Patient verstorben sei. Es wäre sinnvoll, wenn die ZAS hierzu Meldungen an die Stammgemeinschaften verschicken würde, wenn sie Kenntnis von einem Todesfall erhielte. Die *FMH* kritisiert, dass ein elektronisches Patientendossier nicht direkt nach dem Tod einer Patientin / eines Patienten aufgehoben werden dürfe. Nach geltendem Recht könnten Behandlungsfehler bis 10 Jahre nach der Behandlung geltend gemacht werden. Für die Aufhebung sei eine rechtlich kohärente Lösung zu Haftpflichtfragen / Datenaufbewahrung erforderlich. Die *SUVA* fordert die ersatzlose Streichung von Buchstabe c. 6 Kantone[55] fragen, ob ein elektronisches Patientendossier ein gerichtmedizinisches Interesse haben könne. Sie geben zu bedenken, dass das elektronische Patientendossier während einer gewissen Periode (z.B. 10 Jahre) verborgen und nicht veränderbar bestehen bleiben und erst anschliessend vollständig gelöscht werden solle.

Absatz 2: Die *Integic*, die *HL7* und *IHE* wünschen folgenden Zusatz in Absatz 2: „[…] entsprechende Patientendossier sofort entziehen und […]“. Das *KSSG* fragt an dieser Stelle, in welcher Form die Stammgemeinschaften die Gemeinschaften über die Aufhebung des elektronischen Patientendossiers zu informieren hätten. Bislang seien für diesen Prozess keine IHE-Integrationsprofile beschrieben worden, was nachzuholen sei.

Absatz 2 Buchstabe a: *CURAVIVA*, die *Insos* und der Kanton *TG* weisen darauf hin, dass der Begriff der angemessenen Frist zu ungenau sei und schlagen folgenden Wortlaut für Ziffer 1 vor: „[…] ZAS innert einem Monat von der Aufhebung informieren“. Die *HL7* und *IHE* schlagen folgende neuen Ziffern für Buchstabe a vor: „3. die Vernichtung der Daten gemäss Artikel 9 Buchstabe b frühestens 10 Tage und spätestens 60 Tage nach der Aufhebung durchzuführen“ und „4. Auf Gesuch hin die angeordnete Vernichtung der Daten um 60 Tage auszusetzen. Als Gesuchsteller gelten die Patientin oder der Patient, eine Erbengemeinschaft, welche sich mittels Erbbescheinigung ausweisen kann oder ein Willensvollstrecker, der sich mittels Willensvollstreckerzeugnis ausweist.“ Die *medshare* schlägt die identischen, neuen Ziffern vor, jedoch mit dem Unterschied, dass bei Ziffer 3 „frühestens 30 Tage“ gefordert werden. Gemäss *Physioswiss* dürfe der Prozess nicht sein, dass bei der Aufhebung eines elektronischen Patientendossiers alle Gemeinschaften informiert werden. Diese Regelung sei zu streichen und evtl. ein anderer Prozess zu wählen. Eine Streichung fordert auch die *FMH*, welche schreibt, dass die Gemeinschaft durch eine Information der Aufhebung zum Teil erst die Existenz des elektronischen Patientendossiers erfahren würde. Es dürfe keine Löschung in den lokalen Ablagen erfolgen und auch keine der PID. Somit werde auch die Information sowohl an die Gemeinschaft als auch die ZAS hinfällig. Die *Post* gibt zu bedenken, dass nicht klar sei, wie das Löschen des elektronischen Patientendossiers bei allen Gemeinschaften funktioniere. Nur die Stammgemeinschaft müsse das Dossier löschen. Gemäss dem *VGIch* sei der Sinn und Zweck der Informationspflicht an alle Gemeinschaften unklar. Evtl. solle die ZAS – allenfalls automatisiert – andere Gemeinschaften informieren, falls dies notwendig wäre. Ein Widerruf sei zudem grundsätzlich sofort gültig. Zudem sei zu klären, wie die angemessene Frist gemäss Artikel 20 interpretiert werden solle. Die TOZ wiederhole den Begriff der Angemessenheit. Die TOZ sollte technische und organisatorische Zertifizierungsvoraussetzungen enthalten und nicht die Verordnung interpretieren. Es sei ratsam eine Frist (z.B. einen Monat) in der EPDV vorzugeben. Betreffend Buchstabe a Ziffer 2 würde die *Post* folgenden Wortlaut präferieren: „den Nachweis der Widerrufserklärung[…]“. 6 Kantone[56] schreiben, dass im Falle der Beendigung eines elektronischen Patientendossiers der PID, wie bereits bei Artikel 9 erwähnt, bestehen bleiben solle. Somit würde keine Notwendigkeit bestehen, die ZAS zu informieren. Sie schlagen dementsprechend folgenden Verordnungstext von Buchstabe a Ziffer 1 vor: „[…] les communautés dans un délai approprié“. Die *FMH* verweist auf ihren

[55] GE, VS, VD, JU, FR, NE
[56] GE, VS, VD, JU, FR, NE

Kommentar von Artikel 9 und fragt, was „Aufhebung“ bedeute. Zudem sei nicht klar, wie gerichtmedizinische Aspekte im Falle einer Aufhebung nach dem Widerruf der Zustimmung gehandhabt würden.

Absatz 2 Buchstabe b: Die *ÄTG*, die *ASPS* und die *Spitex* wiederholen ihre Stellungnahme von Absatz 1 Buchstabe b. Für die *FMH* erscheint dies nicht praktikabel. Im Falle einer 10-jährigen Nichtnutzung sei auch die Wahrscheinlichkeit, eine Patientin / einen Patienten nicht erreichen zu können nicht gering, weswegen Buchstabe b zu streichen sei, was auch die *SUVA* fordert. 6 Kantone[57] fordern ebenfalls die Streichung von Buchstabe b. Sie schreiben, dass es gut sein könne, dass die Koordinaten (Adresse, Telefonnummer, etc.) nach Ablauf der 10 Jahren der Nichtbenutzung nicht mehr gültig sind. Gemäss *Moeri* sei Buchstabe b obsolet. *SBC* fordert wiederum die Informierung der Patientinnen / Patienten bereits 6 Monate vor der Aufhebung.

3. Abschnitt: Datenlieferung für die Evaluation

Art. 21

[1] Gemeinschaften und Stammgemeinschaften müssen dem BAG regelmässig Daten für die Evaluation nach Artikel 18 EPDG zur Verfügung stellen.

[2] Das EDI legt die zu liefernden Daten fest.

Die *medshare* macht darauf aufmerksam, dass die Artikelüberschrift/-bezeichnung fehle. 7 Stellungnehmende[58] machen geltend, dass die Regelung aus datenschutzrechtlicher Sicht zu präzisieren sei. Das BAG solle nur berechtigt sein, die Daten in anonymisierter Form zu bearbeiten. Die Auflistung in Anhang 6 der EPDV-EDI verdeutliche, dass anonymisierte Daten für die Erhebung der beabsichtigten Informationen problemlos ausreichen würden. Sie sprechen sich dafür aus, Absatz 1 wie bisher zu belassen und Absatz 2 neu als Absatz 3 aufzuführen. Für den neuen Absatz 2 machen sie folgenden Formulierungsvorschlag: „Das BAG darf die Daten nur in anonymisierter Form bearbeiten. Die Gemeinschaften und Stammgemeinschaften sind verpflichtet, die Daten vor der Auslieferung an das BAG zu anonymisieren oder anonymisiert zu lassen“. Ähnlich schreiben der Kanton *ZH* und der *ZAD*, dass dem BAG nur anonymisierte Daten geliefert werden dürften und dass die von Artikel 18 vorgesehene Evaluation keine nicht anonymisierten Daten erfordere. Sie schlagen folgende Ergänzung von Absatz 1 vor: „Gemeinschaften und Stammgemeinschaften stellen dem BAG regelmässig anonymisierte Daten für […]“. Die *Medgate* fragt, wie verlässlich geprüft werden solle, ob Indikatoren Rückschlüsse auf einzelne Gesundheitsfachpersonen oder Patientinnen / Patienten erlauben. Die Datenlieferungen sollen grundsätzlich nur anonymisiert erfolgen. Das *LUKS* und die *FMH* fordern die Begrenzung der Datenlieferungen auf ein absolutes Minimum und fügen an, dass der Aufwand dazu finanziert sein müsse. Gemäss der *FMH* dürfe das elektronische Patientendossier nicht Selbstzweck werden, sondern müsse den im EPDG definierten Zwecken (Art.1, Abs. 3 EPDG) dienen und entsprechende WZW-Kriterien erfüllen. Neben der Anpassung der Verordnung an diese Ziele sei auch ein entsprechendes Evaluationskonzept mit transparenten Kriterien und Indikatoren zu erstellen. Erst danach können und dürfen Evaluationsdaten festgelegt werden. Die in Anhang 6 EPDV-EDI aufgeführten Kennzahlen seien für eine Evaluation der Erreichung der im EPDG festgelegten Zwecke nicht geeignet. *Physioswiss* betont, dass die Kriterien transparent sein müssen. Aus Sicht der *IG eHealth* und *PH CH* sollte Absatz 2 folgendermassen ergänzt werden: „[…] Daten sowie die Fristen für die Einreichung der zu liefernden Daten gemeinsam mit den betroffenen Kreisen fest“. Die *medshare* wünscht ebenfalls die Festlegung von Periodizität und Fristen und die *HL7* sowie die *IHE* schreiben, dass die Periodizität spätestens im Anhang mit den zu liefernden Daten definiert werden müsse. Der *VGIch* schreibt, dass Evaluationsklauseln, welche sich an Bundesbehörden richten, mindestens Angaben zu folgenden Elementen enthielten: Berichterstattende Behörde, Adressat der Ergebnisse der Überprüfung, Zeitpunkt der Überprüfung, Endprodukt, Kriterien der Überprüfung und Gegenstand der Überprüfung. Dieser Regelung werde mit der Vorgabe „regelmässig“ zu wenig Rechnung getragen. Die *SVP* stellt fest, dass die Formulierung offen lasse, in welchem zeitlichen Abstand die Gemeinschaften Daten zur Evaluation einzureichen hätten. Sowohl die Frequenz als auch der Umfang der abzuliefernden Daten seien so festzulegen, dass für die Gemeinschaften kein

[57] GE, VS, VD, JU, FR, NE

[58] privatim, DSBAG, KDSBSON, FR, BE, ZG, AG

unverhältnismässiger Aufwand entstehe. Die *SGMI* kritisiert, dass die weit gefasste Form der Datenlieferung eine Hintertür zur indirekten Kontrolle der Leistungserbringer und zur übermassigen Datensammlung öffne. Die Datenlieferung sei auf ein striktes Minimum im Sinne der anonymen Nutzungsstatistik zu reduzieren. Absatz 2 dürfe nicht zu einem Freipass fürs EDI verkommen. Die *STSAG* bezeichnet Artikel 21 als Blanko-Check und fordern die Verwerfung in dieser Form. Es sei sicherzustellen, dass die Anforderungen nicht beliebig erweitert werden können im EPDV-EDI. Der *VAKA*, die *K3* und der *VZK* weisen darauf hin, dass der Aufbau einer Stammgemeinschaft bereits aufgrund der hohen Anforderungen zur Zertifizierung aufwändig und teuer sei. Mit Artikel 21 würden Stammgemeinschaften weiter finanziell unter Druck gesetzt und hätten keinerlei Nutzen. Der *VAKA* schreibt zudem, dass die Evaluierung des EPDG zwar unbestritten, die Tiefe der Daten und die Ausgabeart jedoch nicht unterstützenswert seien. Deshalb werde die ersatzlose Streichung gefordert. Die *K3* und der *VZK* wünschen eine restriktive Handhabung der Datenanforderungen. Die *SWOR*, der *SBK* und der *SVBG* erachten die vorgesehene Evaluation als besonders wichtig. Sie werde wichtige Anhaltspunkte liefern, um den Verlauf des elektronischen Patientendossiers zu beurteilen und notwenigen Handlungsbedarf aufzuzeigen.

3.1.4 4. Kapitel: Identifikationsmittel

Art. 22	Anforderungen an das Identifikationsmittel
Das Identifikationsmittel muss:	
a.	der Vertrauensstufe 3 der Norm ISO/IEC 29115:2013(E) entsprechen;
b.	so aufgebaut sein, dass es nur von der berechtigten Person verwendet werden kann;
c.	ein Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens zwei Authentifizierungsfaktoren verwenden; und
d.	eine Gültigkeitsdauer von höchstens zehn Jahren aufweisen.

10 Stellungnehmende[59] bezeichnen die Anforderungen an das IDM als sehr hoch. Das Ausführungsrecht solle heute in den Spitälern verwendete IDM zulassen, sofern sie bestimmten Kriterien entsprechen würden. Eine Gesundheitsfachperson in einem Spital sollte nicht mehrere Logins und Zugangssysteme verwalten müssen. Die Anforderungen an das IDM für Gesundheitsfachpersonen in Spitälern seien zu überprüfen. Die *Post* wünscht, dass dort wo Spitalpersonal nach kantonalem Recht gültige IDM einsetze, diese auch für das elektronische Patientendossier verwendet werden sollen. Der *VAKA* verweist ebenfalls auf bereits bestehende IDM-Lösungen und verlangt die Klärung, wo und nach welchen Kriterien diese auch für den Zugriff auf EPDG-Daten verwendet werden können. Ähnlich schreibt der Kanton *LU*, dass das Personal mit neuen, teuren IDM für den Zugriff auf das elektronische Patientendossier ausgerüstet werden müsste, weswegen eine Überarbeitung nötig sei. Die *Medgate* bezeichnet die Anforderungen an die Identitätsbestätigung und das IDM als in vielen Fällen zu hoch und damit zu wenig praktikabel, weshalb vereinfachte Verfahren nötig seien und die *SGMI* schreibt, dass der Einsatz bestehender, bereits weit verbreiteter IDM wünschenswert sei. Die *PKS* weisen darauf hin, dass die Regelungen zu den IDM nicht den im Spital praktizierten Abläufen der Personalabteilung beim Ein- und Austritt von Gesundheitsfachpersonen entsprechen würden. Im Alltag solle auf das vorhandene Authentisierungsverfahren vertraut werden und der Einsatz bestehender, bereits weit verbreiteter IDM sei wünschenswert. Die *IG eHealth*, *PH CH* und *economiesuisse* fordern, dass Artikel 22 mit einer Übergangsbestimmung ergänzt oder wie folgt angepasst werde: „In all jenen stationären Einrichtungen, in welchen die Gesundheitsfachpersonen ein nach kantonalem Recht gültiges IDM für den Zugriff auf Patientendaten einsetzen, kann dieses IDM auch für den Zugriff auf das elektronische Patientendossier verwendet werden“. Der *HÄ CH* und die *ÄTG* plädieren für eine pragmatische und vor allem alltagstaugliche Lösung, was insbesondere hinsichtlich Zeitaufwand und Kosten wichtig sei. Eine einfache Rechtevergabe und Regelung für Praxispersonal sei nötig, damit nicht Sekretariatsaufgaben aufgrund Zugriffsberechtigungen an eine Ärztin / einen Arzt delegiert werden müssten. Gemäss der *K3* und dem *VZK* müsse es möglich sein, dass das System „elektronisches Patientendossier“ dem Spital „vertraue“. Für die Spitäler sei es im Alltag wichtig, dass sie für den Zugriff auf das elektronische Patientendossier nicht wieder auf andere Authentifizierungsverfahren abstützen müssen, sondern das intern verwendete Verfahren nur noch „ergänzt“ werden könne. Dazu müsste das interne Verfahren gewisse Anforderungen erfüllen (z.B. Passwortlänge) und dann beim Zugriff auf das elektronische Patientendossier nur noch mit einem dritten

[59] NW, LU, Post, SZ, ZG, ZH, ZAD, IG eHealth, PH CH, economiesuisse

Faktor ergänzt werden können. Ähnlich macht die *SVP* geltend, dass eine Beschränkung auf einige wenige, konkrete IDM überflüssig sei. In den Einrichtungen bereits vorhandene Authentifizierungsmittel könnten auch für den Zugriff auf das elektronische Patientendossier verwendet werden. Der *VAKA* und der Kanton *AG* weisen darauf hin, dass keine persönliche Vorsprache bei der Registrierung des IDM erforderlich sein solle, da dieser Aufwand viele Patientinnen / Patienten und Gesundheitsfachpersonen abschrecken würde.

Artikel 22 Buchstabe a: Das *BRH* macht darauf aufmerksam, dass die Kontrolle der ISO-Normen über das BAG nicht gewährleistet sei. Daher seien transparente Angaben über die genannten Normen angebracht. Eine einfache Zugänglichkeit sei sicherzustellen und die Kontrollprozesse und –instanzen über diese Normen zu beschreiben. *CURAVIVA*, der *Insos* und der *senesuisse* kritisieren, dass der Verweis auf eine ISO/IEC-Norm unangemessen sei, zumal er das Legalitätsprinzip verletze und auch der Kanton *TG* fragt sich, ob der Verweis auf eine ISO/IEC-Norm auf Verordnungsstufe rechtmässig sei. Weiter schreiben sie, dass dieser Verweis eine Verletzung des Grundsatzes der Transparenz und der Öffentlichkeit der Gesetzestexte nach sich ziehe. Nicht zuletzt sei der Inhalt dieser Normen nur schwer zugänglich. Aus Sicht des Kantons *TG* sei es notwendig, dass die Vertrauensstufe 3 anderen Qualitätsmerkmalen entspreche, welche die EPDV ausdrücklich vorsehe. Dies gelte auch für die Akkreditierung sowie für den Schutz der IDM und für das Verfahren der Authentifizierung. Die *Post* ist ebenfalls der Ansicht, dass nicht eine spezifische Norm auf Stufe Verordnung festgeschrieben werden sollte. Es sollen lediglich die stabilen Anforderungen auf Stufe Verordnung festgelegt werden und einem technisch orientierten Bundesamt sei die entsprechende Kompetenz zu übertragen, um diese detaillierten Anforderungen zu pflegen. Buchstabe a soll gestrichen werden und eine Harmonisierung mit dem Bundesgesetz über die elektronische Signatur (ZertES) sei zu ermöglichen. Gemäss der *ISSS* müsse bei den elektronischen IDM gewährleistet sein, dass diese von den Herausgebern zeitgerecht und in der geforderten Qualität und Menge zur Verfügung gestellt werden können. Dies sei dann möglich, wenn bereits heute bestehende anerkannte und zertifizierte IDM eingesetzt und nicht nach einem anderen Standard neue IDM gefordert würden. Weiter weist die *ISSS* in seiner Stellungnahme auf in der Schweiz und Europa bestehende Mittel für eine sichere Authentisierung hin. Diese würden sich nicht oder nur bedingt nach der ISO/IEC29115 Norm richten. Es wird die Anwendung von bereits definierten elektronischen IDM gewünscht und darauf hingewiesen, dass der eCH-Standard für die Definition weiterer IDM massgeblich sein sollte. Buchstabe a soll neu folgendermassen lauten: „a. einer der folgenden Normen oder Vorschriften entsprechen: - Qualitätsstufe 3 der eCH-0170 Norm; - geregeltes Zertifikat gemäss ZertES; - Suisse ID Authentisierungs-Zertifikat gemäss eCH-0113 Spezifikation; - eIDAS“. Ähnlich fordert die *SQS* die Ersetzung von ISO/IEC29115 mit der elektronischen Signatur nach ZertES.

Artikel 22 Buchstabe c: Die *Post* beantragt eine Präzisierung in der Verordnung, damit hervorgehe, dass mTAN ein mögliches IDM sei. Die *SPO* begrüsst, dass ein Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens 2 Authentifizierungsfaktoren verwendet werden müsse. Die Zugriffssicherheit auf sensible Daten solle mindestens derjenigen der Banken entsprechen. *HIN* begrüsst das dem Sachverhalt angepasste Sicherheitslevel und die strikte Forderung einer 2-Faktor-Authentisierung. Analog dem Niveau, der bei den ambulanten/niedergelassenen Gesundheitsfachpersonen weit verbreiteten IDM, sei die Sicherheitsanforderung auch im stationären Umfeld anzuwenden. Als IPD würden sie über entsprechende Lösungen und Erfahrungen für den Einsatz in grossen stationären Institutionen verfügen. Die *SGMI* plädiert wiederum dafür, dass von einer zweistufigen Authentifizierung abgesehen werde.

Artikel 22 Buchstabe d: 6 Stellungnehmende[60] machen geltend, dass eine Gültigkeit von höchstens 10 Jahren in Anbetracht der stets voranschreitenden Weiterentwicklung der Technik sehr lang erscheine. Den Erläuterungen würden sich zu diesem Punkt leider keine Hintergrundüberlegungen entnehmen lassen. Sie fordern die Überprüfung der Maximalfrist von 10 Jahren. Der *DSBAG* schlägt konkret eine Festlegung der Maximalfrist auf 2 Jahre vor, der Kanton *BE* eine auf deren 5. Der *VAKA* und die *Post* fordern die Streichung dieser Anforderung. Würde hingegen eine zeitliche Komponente als notwendig erachtet, so solle dies gemäss der *Post* in Artikel 25 geregelt und mit anderen Gesetzen vereinheitlicht

[60] DSBAG, privatim, KDSBSON, FR, ZG, BE

werden.

Art. 23 Identitätsprüfung
[1] Der Herausgeber des Identifikationsmittels muss die Identität der antragstellenden Person überprüfen. Diese muss sich mit einem Ausweis nach dem Ausweisgesetz vom 22. Juni 2001 oder einem Ausweis nach den Artikeln 41–41b des Ausländergesetzes vom 16. Dezember 2005 ausweisen oder einen mit einer qualifizierten elektronischen Signatur nach dem Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur signierten Antrag auf elektronischem Weg einreichen.
[2] Wird das Identifikationsmittel für die Authentifizierung einer Gesundheitsfachperson verwendet, so muss zusätzlich überprüft werden, ob es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt.
[3] Die Prüfung der Identität der antragstellenden Person nach Absatz 1 und der Qualifikation einer Gesundheitsfachperson nach Absatz 2 kann an Dritte delegiert werden.

Die *PKS* und die *SGMI* bemängeln, dass analog Artikel 22 auch für die Identitätsprüfung zu hohe Hürden definiert worden seien. Es solle auf bewährte und gut etablierte Methoden zurückgegriffen werden. Die *Post* kritisiert wiederum, dass die in diesem Entwurf vorgeschlagenen, sehr hohen Anforderungen an die IDM im Widerspruch zu den sehr tiefen Anforderungen an die Identitätsprüfung stünden. Sie beantragt, dass die gleichen Anforderungen gelten, wie sie im Entwurf der in Revision befindenden VZertES für die Ausstellung von geregelten Zertifikaten festgehalten werden. Gemäss der *STSAG* sei die Identitätsprüfung pragmatischer zu lösen. Es sollte reichen, wenn die Identität durch die Institution per se geprüft werde (mit dem Anstellungsverhältnis), die Rolle definiert werde (z.B. im KIS) und mittels einer technischen Validierung (z.B. HIN access gateway) der Zugriff ermöglicht werde. Die Identifizierung / Authentifizierung im Primärsystem, gekoppelt mit einer gesicherten Zugangsinfrastruktur, könne im Sinne der 2-Faktor-Authentifizierung genutzt werden, um ohne weitere Identitätsabfragen zum elektronischen Patientendossier einer gewissen Person zu gelangen.

Absatz 1: Die *Medgate* wiederholt ihren Kommentar zu Artikel 22. 6 Kantone[61] machen folgenden Formulierungsvorschlag für Artikel 23 Absatz 1: „L'éditeur ou la communauté est tenu de vérifier l'identité de la personne qui demande un moyen d'authentification". Die *ISSS* schreibt, dass die Definition der Anforderungen an die Identitätsprüfung Bestandteil der jeweiligen Norm/Regelung (eCH-0170, eCH-0113, ZertES, eIDAS) sei und schlägt folgenden Wortlaut für Absatz 1 vor: „[…] antragsstellenden Person gemäss der jeweiligen Norm, unter der das IDM herausgegeben wird, überprüfen. […]". Der *Spitex* und die *ASPS* machen darauf aufmerksam, dass viele Spitex-Klienten/innen im hohen Alter nicht mehr über eine gültige Identitätskarte oder einen Führerschein verfügen würden. Eine Neubeschaffung sei für die Personen oftmals sehr umständlich, weswegen eine andere Identifikationsmöglichkeit vorzusehen sei. Die *Tessaris* weist darauf hin, dass bei der Identitätsprüfung analog zu Artikel 5 Absatz 2 für Personen, die sich in der Schweiz aufhielten und nicht über eine Versichertennummer verfügen auch andere Mittel zum Nachweis der Identität zugelassen werden.

Absatz 2: Der *VAKA* schreibt, dass an dieser Stelle von einer Prüfung ausgegangen werde, bei welcher weder das Verfahren noch die Datenlage geklärt sei. Das BAG müsse klar definieren, wie eine solche Prüfung abzulaufen habe. Der *Spitex* und die *ASPS* machen darauf aufmerksam, dass solange nicht alle Pflegefachpersonen in einem Register registriert seien, die Identifikation nach Artikel 2 Buchstabe b EPDG sehr aufwändig sei. Die Verordnung müsse entsprechende Register für die Gesundheitsberufe vorsehen resp. regeln. Die *FMH* fordert, dass es nicht nur ein Attribut „Gesundheitsfachperson" geben dürfe, sondern die verschiedenen Berufsgruppen zu unterscheiden seien. Ähnlich schreibt *HIN*, dass das Attribut „Gesundheitsfachperson" zusätzlich und in Zusammenarbeit mit den Berufsverbänden mit dem entsprechenden Typ des Medizinalberufes zu ergänzen sei.

Absatz 3: Gemäss der *K3* und dem *VZK* sei Absatz 3 so auszulegen, dass ein Spital oder ein Pflegheim seine Mitarbeitenden identifizieren und zusätzlich auch prüfen könne, ob es sich um eine Gesundheitsfachperson handelt. Alles andere sei nicht praktikabel und viel zu teuer. Die *SBK* und die *SWOR* begrüssen die Vergabe der GLN an Gesundheitsfachpersonen. Den Lösungsansatz würden sie in der

[61] FR, NE, VS, VD, JU, GE

Führung eines nationalen Berufsregisters für Gesundheitsfachpersonen sehen. Die *FMH* lehnt die Delegation der Überprüfung der Qualifikation einer Gesundheitsfachperson an beliebige Dritte ab, da es ein nicht tolerierbares Risiko sei. Die Verantwortung solle bei bestimmten, qualifizierten Stellen bleiben, deren Anforderungen zu definieren seien.

Art. 24 Daten des Identifikationsmittels

[1] Der Herausgeber des Identifikationsmittels erfasst folgende Daten anhand des vorgelegten Identitätsnachweises der antragstellenden Person:

a. den Namen;
b. die Vornamen;
c. das Geschlecht;
d. das Geburtsdatum;
e. die Nummer des Identitätsnachweises nach Artikel 23 Absatz 1.

[2] Er kann bei Gesundheitsfachpersonen zusätzlich die eindeutige Identifikationsnummer (GLN) erfassen.

[3] Er kann die Angaben nach den Absätzen 1 und 2 zur Identifizierung an die Zugangsportale übermitteln.

[4] Er informiert die antragstellende Person über die Sicherheitsvorkehrungen, die sie im Umgang mit dem Identifikationsmittel treffen muss.

Die *Post* weist bezüglich des ersten Absatzes darauf hin, dass in der Liste der Attribute die AHVN13 fehle. Dieses Attribut solle von der IDP nur für das elektronische Patientendossier zur Verfügung gestellt werden und nicht für andere Zwecke. Ohne diese Angaben gebe es keine Vereinfachung im Registrationsprozess für Patientinnen / Patienten. Würden diese Anforderungen nicht heraufgesetzt, müssten sie ihre komplexen Registrationsprozesse beibehalten und würden wenig profitieren. Das bedeute viel Kosten für IDM ohne zusätzlichen Wert. Die *Post* beantragt, dass mindestens eine Möglichkeit für die Erfassung erlaubt werde. Diese dürfe auch bei einer Identitätsprüfung, die nicht im Rahmen des elektronischen Patientendossiers erfolge, erhoben werden, dürfe aber nur im Zusammenhang mit dem elektronischen Patientendossier genutzt werden. Betreffend Absatz 1 Buchstabe e schreibt die *Post* zudem, dass nicht nur die Nummer des Identitätsnachweises erfasst werden sollte, sondern auch der Typ des Dokuments und schlägt vor, dass in der Definition der Metadaten eine Codierung für die Identitätsnachweise erfasst werden sollte. Die *FMH* spricht sich bezüglich Buchstaben e dafür aus, dass die Nummer des Identitätsnachweises mit der GLN zu ersetzen sei. Absatz 2 sei zudem zu streichen. Die *Tessaris* wiederholt ihren Kommentar von Artikel 23 Absatz 1 in Bezug auf den Buchstaben e. 6 Kantone[62] weisen darauf hin, dass das IDM zwar zu kontrollieren sei, die Nummer jedoch nicht registriert werden müsse. Das wäre verlorene Zeit und es gebe keinen Grund, diese Daten zu speichern. Sie fordern die Streichung von Buchstabe e. Gemäss der *Tessaris* sei die in Absatz 4 vorgeschlagene Informationspflicht analog zu den Bemerkungen zu Artikel 14 Absatz 2 mit einem gewissen Haftungsrisiko für den Herausgeber des IDM verbunden. Es sei zudem auch auf die Haftungsregel nach Artikel 59a OR für die Inhaber von Signaturschlüssel hinzuweisen.

Art. 25 Erneuerung der Gültigkeitsdauer des Identifikationsmittels

[1] Das Identifikationsmittel kann vor Ablauf seiner Gültigkeitsdauer erneuert werden.

[2] Der Herausgeber überprüft bei der Erneuerung des Identifikationsmittels nach Artikel 23 die Identität der antragstellenden Person.

Gemäss 6 Kantonen[63] gebe es eine Verwirrung zwischen Identifizierung und Authentifikation. Artikel 25 sei folgendermassen anzupassen: „Renouvellement de la durée de validité du moyen d'authentification. 1. Le moyen d'authentification peut être renouvelé avant l'expiration de sa durée de validité. 2. Lors du renouvellement du moyen d'authentification, l'éditeur ou la communauté vérifie à nouveau l'identité du demandeur conformément à l'art. 23". Der *HÄ CH* und die *ÄTG* schreiben, dass die Gültigkeitsdauer aus rationellen Gründen zur Minimierung von Umtrieben und Kosten möglichst lange (keinesfalls unter 3, minimal 2 Jahren) sein sollte.

62 GE, FR, VS, VD, JU, NE
63 GE, FR, VS, VD, JU, NE

Absatz 2: Der *VAKA* macht geltend, dass wenn die Person über Artikel 23 Absatz 1 bereits einmal mit einem Ausweis identifiziert worden sei, eine Erneuerung keine neue Ausweisprüfung bedürfe. Die nochmalige Ausweisprüfung sei ersatzlos zu streichen. Eine Streichung wünschen auch das *LUKS*, die *FMH* und die *SGMI*. Gemäss 8 Stellungnehmenden[64] sei eine erneute Überprüfung der Person überflüssig, wenn ein IDM noch Gültigkeit habe. Die *IG eHealth* und *PH CH* schlagen folgende Änderung in Absatz 2 vor: „Verliert ein IDM seine Gültigkeit, so muss der Herausgeber des Identifikationsmittels für dessen Erneuerung nach Artikel 23 die Identität der antragstellenden Person neu überprüfen".

Art. 26	Sperrung des Identifikationsmittels
Das Identifikationsmittel kann von der Inhaberin oder dem Inhaber jederzeit unwiderruflich gesperrt werden.	

6 Kantone[65] weisen darauf hin, dass die Inhaberin / der Inhaber für die Sperrung die Gemeinschaft anfragen müsse. Er könne dies nicht selber machen. Sie fordern folgenden Titel für Artikel 26: „Blocage du moyen d'authentification" und folgenden Wortlaut des Artikels: „Le titulaire du moyen d'authentification peut demander de bloquer celui-ci à tout moment". Gemäss dem *HÄ CH* und der *ÄTG* müsse hier genauer spezifiziert werden, der Nutzer brauche eine Sicherheit. Der Aufwand für eine Erneuerung und einen Anbieterwechsel müsse begrenzt werden. Für *SCH* ist Artikel 26 zu restriktiv. Es sollte bei den IDM geregelt sein. Unter Umständen würde das IDM auch für andere Anwendungen genutzt. Artikel 26 sei zu streichen und bei Bedarf in Anhang 5 zu übertragen. Die *Tessaris* weist darauf hin, dass für die Form des Widerrufes nichts vorgesehen sei, womit Telefon, SMS oder E-Mail ausreichen müsste. Da die Sperrung gemäss Gesetzeswortlaut „unwiderruflich" erfolge, sei zudem unklar, wie die Inhaberin / der Inhaber bei einer Sperrung infolge Verlust oder Diebstahl des IDM vorzugehen habe. Gemäss *HIN* sei zu fordern, dass bei jedem Einstieg ins elektronische Patientendossier das IDM auf eine Revokation (Ungültigkeitserklärung) überprüft werde. Es reiche nicht, nur beim IDP die Sperrung zu regeln. Artikel 26 sei folgendermassen zu ergänzen: „Der Herausgeber führt eine Liste der gesperrten oder für ungültig erklärten IDM (Revokationstabelle). Die Gemeinschaft prüft bei jedem Zugriff, ob die Person korrekt authentisiert wurde und deren ID-Mittel nicht revoziert ist". Die *Post* bemängelt, dass die Beschreibung unvollständig sei. Der Herausgeber selbst könne IDM sperren, wenn er glaubhaft informiert werde, dass die Angaben nicht mehr stimmen. Es bestehe die Gefahr, dass falsche Erwartungen geweckt würden. Der Herausgeber müsse das IDM auch sperren können, wenn er oder der Inhaber mindestens den Verdacht habe, dass ein Missbrauch vorliege, weswegen Gründe für die Sperrung aufgelistet werden sollten. Falls der Herausgeber des IDM sich vergewissern müsse, dass die Person, welche die Sperrung beantragt, dazu berechtigt ist, müsse dies zudem explizit erwähnt werden. Des Weiteren wäre eine Information des Inhabers nach der Sperrung eines IDM wünschenswert, damit dieser die Möglichkeit hätte, nicht gewünschte Sperrungen zu erkennen.

3.1.5 5. Kapitel: Akkreditierung

Art. 27	Anforderungen
[1] Die Akkreditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung (AkkBV) vom 17. Juni 1996 sowie ISO/IEC 27006:201510, soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.	
[2] Je eine separate Akkreditierung ist erforderlich für die Zertifizierung von:	
a.	Gemeinschaften und Stammgemeinschaften;
b.	Herausgeber von Identifikationsmitteln.
[3] Die Zertifizierungsstellen müssen neben den Voraussetzungen nach der AkkBV über eine festgelegte Organisation sowie ein festgelegtes Kontrollverfahren verfügen. Darin müssen insbesondere geregelt sein:	
a.	die Begutachtungs- oder Prüfkriterien, mit denen die Einhaltung der Zertifizierungsvoraussetzungen überprüft werden;
b.	der Ablauf des Verfahrens, insbesondere das Vorgehen bei festgestellten Unregelmässigkeiten;
c.	die Verwendung des vom BAG zur Verfügung gestellten Zertifizierungssystems zur Prüfung der Datenübertragung von Gemeinschaften und Stammgemeinschaften.
[4] Das EDI legt die Mindestanforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt, fest.	

[64] LUKS, FMH, SGMI, HL7, IHE, Integic, IG eHealth, PH CH

[65] GE, FR, VS, VD, JU, NE

Das *LUKS* betrachtet die Anforderungen an Zertifizierungsstellen als zu hoch und fordert deren Reduktion auf ein praktikables Minimum. Gleiches wünschen die *PKS*, die *SGMI* und die *FMH*. Sie schreiben, dass die hohen Anforderungen zu überhöhten Kosten der Akkreditierung führen würden, ohne die Sicherheit des Gesamtgebildes wesentlich zu verbessern. Die *STSAG* plädiert dafür, dass die Anforderungen der Gemeinschaften über die Stammgemeinschaften definiert und geprüft und nicht über eine Akkreditierungsgesellschaft gelöst werden sollten. Für Stammgemeinschaften sollte eine Akkreditierung, für Gemeinschaften nur eine Zertifizierung vorgesehen werden.

Die *BRH*, *CURAVIVA*, der *Insos* sowie der Kanton *TG* wiederholen bezüglich Artikel 27 Absatz 1 ihre Stellungnahmen von Artikel 22 Buchstabe a und der *senesuisse* seinen von Artikel 22 Buchstabe b. Die *SQS* weist darauf hin, dass Datenschutz und Datensicherheit für das elektronische Patientendossier von zentraler Bedeutung seien. Gemäss dem erläuternden Bericht zum EPDG solle die Einhaltung durch ein Zertifizierungsverfahren sichergestellt werden. Dabei sei vor allem auch an das Zertifizierungsverfahren nach Artikel 11 DSG zu denken. Gerade in diesem Bereich sei für eine zielführende Umsetzung wichtig, dass international anerkannte Grundsätze und Verfahren zur Anwendung kämen. Die Zertifizierung VDSZ erfülle diesen Anspruch, indem die international anerkannte ISO/IEC 27001 in weiten Teilen bezüglich der Aspekte der Informations-/Datensicherheit gemäss Ziffer 3 der Richtlinien über die Zertifizierung von Organisationen und Verfahren enthalten sei und die Anforderungen des Datenschutzes/Datenschutzmanagementsystems Teil dieses spezifischen Zertifikats seien. Die Akkreditierung der Zertifizierungsstellen sei in der VDSZ geregelt, ebenso die Anforderungen an das Personal. Des Weiteren habe sich die VDSZ-Zertifizierung in den vergangen Jahren im Rahmen der gesetzlich zwingenden Zertifizierungen der Datenannahmestellen der sozialen Krankenversicherungen bewährt. Die *SQS* fordert folgende Änderung von Artikel 27 Absatz 1: „[…] sowie nach der Verordnung für Datenschutzzertifizierungen (VDSZ) vom 28. September 2007, soweit […]“.

Im Rahmen von Absatz 3 schreibt die *SQS*, dass zusätzlich zur Anwendung der Akkreditierung- und Bezeichnungsverordnung (AkkBV) auch die Anwendung ISO/IEC 27006:2015 gefordert werde. Hier seien die Forderungen redundant und der Artikel sollte von unnötigen Anforderungen befreit werden. Die ISO/IEC 27006 sei nur relevant, wenn nach ISO/IEC 27001 zertifiziert werden müsse. Artikel 27 Absatz 3 Buchstaben a und b seien ersatzlos zu streichen. Bezüglich des Absatzes 4 weist die *SQS* darauf hin, dass auch die Anforderungen an die Qualifikation durch die Akkreditierung gegeben seien. Die in Anhang 7 geregelten technischen und organisatorischen Voraussetzungen resp. Anforderungen für Stammgemeinschaften und Gemeinschaften würden keine Inhalte aufweisen, welche den Anforderungen nach ISO/IEC 27001:2013 oder den Anforderungen einer Zertifizierung nach Artikel 11 DSG abweichen und spezifische Kenntnisse in Medizininformatik bedingen würden, um eine regelkonforme Überprüfung im Rahmen der Zertifizierung zu garantieren. Absatz 4 sei deshalb ebenfalls ersatzlos zu streichen.

Art. 28	Akkreditierungsverfahren
Die Schweizerische Akkreditierungsstelle zieht für das Akkreditierungsverfahren und die Nachkontrolle sowie für die Sistierung oder den Entzug einer Akkreditierung das BAG bei.	

Gemäss der *FMH* dürfe es nicht sein, dass für die Akkreditierungsverfahren viel Zeit und Geld aufgewendet werden müsse, gerade wenn man möchte, dass unabhängige Ärztegesellschaften Gemeinschaften bilden.

3.1.6 6. Kapitel: Zertifizierung

1. Abschnitt: Zertifizierungsvoraussetzungen

Art. 29	Gemeinschaften und Stammgemeinschaften
[1] Mit dem Zertifizierungsverfahren wird geprüft, ob eine Gemeinschaft die Zertifizierungsvoraussetzungen nach den Artikeln 8–12 oder eine Stammgemeinschaft die Zertifizierungsvoraussetzungen nach den Artikeln 8–20 erfüllt.	
[2] Das EDI regelt die Einzelheiten der Zertifizierungsvoraussetzungen.	

[3] Das BAG passt die Zertifizierungsvoraussetzungen dem Stand der Technik an.

[4] Für den Erlass der Einzelheiten nach Absatz 2 und für die Anpassungen nach Absatz 3 werden die interessierten Kreise angehört.

Der *VAKA* wiederholt an dieser Stelle den Kommentar zu Artikel 18. Die *IG eHealth*, *PH CH* und die *Post* weisen darauf hin, dass das EPDG ein starres System beschreibe. Viele technische Vorgaben würden durch das EDI vorgegeben. Der vorliegende Erlassenstext beschreibe allerdings nirgends wie Anpassungsprozesse vorgenommen und garantiert werden. Während die *IG eHealth* und *PH CH* vorschlagen, den Erlassenstext durch einen neuen Abschnitt „Systemanpassungen" zu ergänzen, spricht sich die *Post* für die Aufnahme eines neuen Artikels „Anpassungsklausel" aus. Die *Post* fügt an, dass ein Organ zu definieren sei, das Anpassungen vornimmt. Zudem müsse ein Prozess beschrieben werden, wie Änderungen unter welchen Fristen auf- und angenommen sowie umgesetzt werden. Die Gemeinschaften und die Industrie seien im Prozess zu beteiligen. Für die *FMH* sind die Zertifizierungsvoraussetzungen zu hoch.

Absatz 3: *CURAVIVA* und der *Insos* kritisieren, dass die Delegation von Kompetenzen mit ebenso vagem Inhalt im Hinblick auf die Erfordernisse des Legalitätsprinzips unannehmbar sei. Ähnlich schreibt der Kanton *TG*, dass die Delegation der Anpassungen der Zertifizierungsvoraussetzungen an das BAG zu umfassend und zu vage sei. Gemäss dem Kanton *ZH* und des *ZAD* sei es problematisch, dass das EDI gemäss Absatz 3 die Vorgaben festlege, das BAG jedoch diese dem Stand der Technik anpassen könne. Sachgerecht wäre, dass das EDI auch die Bestimmungen anpasse. Nach Artikel 12 Absatz 2 EPDG sei eine Ermächtigung des BAG zulässig. Nach dem Grundsatz „a maiore minus" müsse auch eine Ermächtigung des EDI zulässig sein. Während der Kanton *AG* die Kompetenzdelegation an das BAG zur Anpassung der Zertifizierungsanpassungen an den Stand der Technik begrüsst, fordert die *FMH* die Ersetzung dieser Delegation durch eine generelle, funktionale Anforderungsbeschreibung auf Ebene Bundesratsverordnung. Die Voraussetzungen seien zudem auf das erforderliche Mindestmass für die Bildung eines Vertrauenraums zu beschränken.

Art. 30 Herausgeber von Identifikationsmitteln

[1] Die Herausgeber von Identifikationsmitteln müssen:

a. in der Lage sein, Identifikationsmittel gemäss den Anforderungen nach den Artikeln 22–26 herauszugeben und zu verwalten;

b. sicherstellen, dass das Personal über die erforderlichen Fachkenntnisse, Erfahrungen und Qualifikationen verfügt;

c. Informatiksysteme und -produkte verwenden, die vertrauenswürdig sind und zuverlässig betrieben werden;

d. Datenschutz und Datensicherheit mit geeigneten organisatorischen und technischen Massnahmen gewährleisten und die entsprechenden Kontrollen sicherstellen.

[2] Das EDI erlässt Vorgaben für den Schutz der Identifikationsmittel und für das Verfahren zu deren Authentifizierung. Sie richten sich nach ISO/IEC 15408:200911 und entsprechen der Evaluierungsstufe 2.

[3] Das EDI regelt die Einzelheiten der Zertifizierungsvoraussetzungen. Das BAG kann dazu Empfehlungen erlassen.

[4] Das BAG passt die Zertifizierungsvoraussetzungen dem Stand der Technik an.

[5] Für den Erlass der Einzelheiten nach Absatz 3 und für die Anpassungen nach Absatz 4 werden die interessierten Kreise angehört.

Die *BRH* wiederholt an dieser Stelle ihren Kommentar zu Artikel 22 Buchstabe a und Artikel 27 Absatz 1, die *Post* ihre Stellungnahme von Artikel 22 Buchstabe c. *HIN* macht geltend, dass die Rolle des Herausgebers des Identifikationsmittels zu ungenau sei. Im IHE-Kontext spreche man im Thema Authentisierung und Zugriffsregelung vom IDP, ATP und dem STS. In der aktuellen Ausführung sei nicht klar, ob im Herausgeber alle drei Rollen integriert seien oder nicht. Das für jede Transaktion notwendige XUA-Token beinhalte Daten, welche von allen drei Rollen beigesteuert werden: Authentisierungsinformationen (IDP), Attribut Gesundheitsfachperson (ATP) und die restlichen Angaben für das Token (IDs, Rolle etc.), welche vom STS kämen. Würden diese drei Rollen unterschieden und würde unter dem Herausgeber des IDM nur der IDP gesehen, ergäbe das eine sicherheitstechnische Lücke, denn der STS und ATP würden nicht zertifiziert und geprüft, steuern jedoch sicherheitsrelevante Daten bei. *HIN* schlägt vor, in Artikel 30 die Rolle des Herausgebers der ID zu ergänzen: „Ein Herausgeber des IDM muss alle notwendigen Aktoren (IDP, ATP und STS) zur Verfügung stellen, die nötig sind, eine gültige

Authentisierung zu ermöglichen“.

Absatz 1: Die *Post* bezeichnet Absatz 1 als sinnvoll und wünschenswert. Der Kanton *NW* schreibt an dieser Stelle, dass die Zertifizierungsstelle jährlich für alle Gemeinschaften überprüfe, ob deren Zertifizierungsvoraussetzungen noch erfüllt seien. Dies sei zu aufwändig, zumal die Zertifikate gemäss Artikel 34 3 Jahre gültig sein sollen. Diese Überprüfungen sollen während der dreijährigen Geltungsdauer der Zertifikate nicht generell jährlich, sondern nur stichprobenweise erfolgen. Die *ISSS* macht betreffend Buchstabe b folgenden Präzisierungsvorschlag: „[…] Qualifikationen und anerkannte Zertifizierungen verfügt“. Buchstabe c sei in Ergänzung zu Artikel 11 Absatz 4 zudem folgendermassen anzupassen: „[…] zuverlässig in der Schweiz betrieben werden“.

Absatz 2: Der *senesuisse* wiederholt an dieser Stelle seinen Kommentar zu Artikel 22 Buchstabe b und Artikel 27 Absatz 1, die *Post* und *CURAVIVA* ihre Stellungnahmen von Artikel 22 Buchstabe a und ebenfalls Artikel 27 Absatz 1. Die *Post* schreibt zudem, dass dieser Absatz unklar zu verstehen sei, denn IDM dienten der Authentifizierung. Es würde die Lesbarkeit der Verordnung erhöhen, wenn alle Anforderungen an das IDM an einem Ort geregelt würden. Sofern es auf Stufe Verordnung Sinn mache, empfiehlt die *Post* diesen Absatz nach Artikel 22 zu verschieben. Die *FMH* kritisiert, dass die Vorgaben zum Schutz des IDM bereits in Artikel 22 Buchstabe a mit der ISO/IEC 29115:2013(E) definiert seien. Ein weiterer Schutz sei nicht erforderlich, weshalb Absatz 2 zu streichen sei.

Absätze 3 - 5: Gemäss der *Post* ist unklar, ob mit Absatz 3 die Zertifizierungsanforderungen an den Herausgeber oder an die Zertifizierungsstelle gemeint seien. Die in Anhang 7 (Art. 7) EPDV-EDI in Kapitel 2 erwähnten Anforderungen könnten direkt hier erwähnt werden womit sich die Absätze 3 bis 5 erübrigen würden. Die *FMH* weist darauf hin, dass das EDI Einzelheiten der Zertifizierung regeln könne, aber nur auf Basis der ISO-Norm gemäss Artikel 22 Buchstabe a. Es dürften keine darüber hinausgehenden Anforderungen gestellt werden. Absatz 3 solle folgendermassen lauten: „[…] Zertifizierungsvoraussetzungen gemäss Artikel 22 Buchstabe a“. *CURAVIVA* und der Kanton *TG* wiederholen betreffend Absatz 4 ihre Stellungnahmen von Artikel 29 Absatz 3.

2. Abschnitt: Zertifizierungsverfahren

Art. 31 Ablauf

[1] In einem Voraudit prüft die Zertifizierungsstelle, ob der Gesuchsteller oder die Gesuchstellerin auf das Kontrollverfahren vorbereitet ist, und beurteilt und dokumentiert dessen oder deren Unterlagen.

[2] Im anschliessenden Zertifizierungsaudit überprüft sie anhand ihrer Begutachtungs- oder Prüfkriterien die Wirksamkeit der durch die Gesuchstellerin oder den Gesuchsteller getroffenen Massnahmen.

[3] Sie erteilt das Zertifikat, wenn Voraudit und Zertifizierungsaudit zum Ergebnis führen, dass die Gemeinschaft, die Stammgemeinschaft oder der Herausgeber von Identifikationsmitteln die jeweiligen Anforderungen nach den Artikeln 8–12, 8–20 oder 22–26 erfüllen.

Die *Post* ist der Ansicht, dass die in Artikel 27 Absatz 1 erwähnte AkkBV für eine Zertifizierung ausreichend sein sollte und Artikel 31 somit zu streichen sei. Während die skizzierten Zertifizierungsetappen für den Kanton *AG* sinnvoll erscheinen, schreibt die *FMH* wiederum, dass die Zertifizierungsanforderungen zu hoch seien und auch das Zertifizierungsverfahren nicht überreguliert werden sollte. Konkret wird die Streichung von Artikel 31 gewünscht. Die *SQS* weist darauf hin, dass im zweiten Abschnitt EPDV zum Zertifizierungsverfahren Angaben zu Fristen fehlen, welche für die Sistierung sowie für den definitiven Entzug gelten würden. Falls die Stammgemeinschaften und Gemeinschaften nach einer bestehenden Norm zertifiziert würden, so seien die Fristen im Rahmen der Norm geregelt. Zwei Varianten seien möglich, je abhängig davon, welche Zertifizierungsnorm gewählt wird oder ob ein eigenes Zertifizierungsverfahren für die Zertifizierungen im Bereich des elektronischen Patientendossiers in der EPDV geregelt werde. Sistierung sowie Entzug einer Zertifizierung durch die Zertifizierer bei festgestellten Unregelmässigkeiten und Hauptabweichungen würden sich unmittelbar auf die Zulassung der Spitäler sowie anderer Einrichtungen und damit auf die Durchführung des KVG auswirken. Aus diesem Grund seien für die Regelung der Verfahrensfristen bei einem Entzug oder einer Sistierung der Zertifizierung die Bedingungen des öffentlichen Verfahrensrechts zu beachten. Dies spreche dafür, dass die Fristen

in der EPDV spezifisch geregelt werden. Die beiden Verfahren im Zusammenhang mit Sistierung und Entzug von Zertifizierungen, einerseits nach öffentlichem Recht bezüglich der Zulassungsbedingungen des KVG, andrerseits nach den Regelungen der Zertifizierung gemäss ISO-Normen würden sich in keiner Art und Weise bezüglich Fristen und Rechtsweg entsprechen. Ausgehend davon sei eine Regelung der Fristen im Rahmen der Zertifizierungsbedingungen im 2. Abschnitt EPDV von zentraler Bedeutung und müsse verhältnismässig sein.
Variante a bedinge folgenden, zusätzlichen Absatz in Artikel 31: „Das Zertifizierungsverfahren von Stammgemeinschaften und Gemeinschaften richtet sich nach der Verordnung über die Datenschutzzertifizierungen (VDSZ) vom 28. September 2007, soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält". Bei der Variante b ginge es darum, im Rahmen des zweiten Abschnittes „Zertifizierungsverfahren" von Kapitel 6 EDPV, Bestimmungen bezüglich Fristen für die Behebung von Hauptabweichungen sowie Sistierung und Entzug einzufügen. Die *OFAC* weist darauf hin, dass sie bereits seit 2009 Erfahrung in der ISO 27001-Zertifzierung sowie der VDSZ habe. Die Überlagerung der ISO 29115-Normen, der Anforderungen, die spezifisch für die eID der Leistungserbringer im Gesundheitsbereich gelten, sowie die Konformität der Profilschutz der eID, bedeuten ein normatives (Volumen) und ein Zertifizierungsvolumen (in Audittagen), welches über die Zeit und mit einer zu definierenden Zeitdauer verteilt werden müsse. Es bedürfe an Übergangsbestimmungen in diesem Bereich.

Art. 32 Meldung an das BAG

[1] Die Zertifizierungsstelle teilt dem BAG jedes erteilte und erneuerte Zertifikat sowie Sistierungen oder Entzüge von Zertifikaten innert angemessener Frist mit und stellt die für den Eintrag in den Abfragedienst für die zertifizierten Gemeinschaften und Stammgemeinschaften nach Artikel 39 notwendigen Daten zur Verfügung.

[2] Das BAG veröffentlicht ein Verzeichnis der erteilten Zertifikate.

CURAVIVA, der *Insos* und der Kanton *TG* wiederholen ihre Stellungnahmen von Artikel 20 Absatz 2 Buchstabe a. Die *Post* bezeichnet Artikel 32 als sinnvoll.

Art. 33 Überwachung

[1] Die Zertifizierungsstelle hat jährlich zu überprüfen, ob die Zertifizierungsvoraussetzungen weiterhin erfüllt sind.

[2] Stellt die Zertifizierungsstelle im Rahmen ihrer Überwachungstätigkeit wesentliche Abweichungen von den Zertifizierungsvoraussetzungen fest, beispielsweise betreffend die Erfüllung von Bedingungen oder Auflagen, so informiert sie das BAG.

Die *GDK*, der *ZAD* sowie 11 Kantone[66] weisen darauf hin, dass die Zertifizierungsstelle jährlich für alle Gemeinschaften überprüfe, ob deren Zertifizierungsvoraussetzungen noch erfüllt seien. Dies sei zu aufwändig, zumal die Zertifikate gemäss Artikel 34 3 Jahre gültig sein sollen. Diese Überprüfungen sollen während der dreijährigen Geltungsdauer der Zertifikate nicht generell jährlich, sondern nur stichprobenweise erfolgen. Den gleichen Vorschlag machen auch die *K3* und der *VZK*. Der Kanton *ZG* fügt dazu, dass Überprüfungen auch bei Verdacht oder Hinweisen vorgenommen werden sollten. Ähnlich schlägt der Kanton *AI* folgenden Wortlaut für Absatz 1 vor: „Die Zertifizierungsstelle hat stichprobenweise oder bei Verdacht zu überprüfen, ob die Zertifizierungsvoraussetzungen weiterhin erfüllt sind" und die *Insel* plädiert für folgenden Text: „Bei begründetem Verdacht, dass die Zertifizierungsvoraussetzungen nicht mehr eingehalten werden, kann das BAG eine Überprüfung durch die Zertifizierungsstelle anordnen". Die *FMH* sieht in der jährlichen Überprüfung einen zu hohen Aufwand resp. zu hohe Kosten und schlägt eine mindestens dreijährige Frist vor. Aus Sicht der *Post* sollte zudem eine Überprüfung alle 2 Jahre genügen. Für die Zertifizierung der IDM mache jährlich Sinn. Die *BFH* fragt, wieso bei einer jährlichen Überprüfung das Zertifikat nicht jeweils um 1 Jahr verlängert werde. Es mache auch keinen Sinn, im dritten Jahr eine Überprüfung durchzuführen, wenn das Zertifikat ablaufe und ohnehin eine Rezertifizierung vorgenommen werden müsse. Gemäss dem Kanton *AG* seien die jährliche Überwachung und die dreijährige Rezertifizierung in den Erläuterungen besser voneinander abzugrenzen. Es seien auch die Begriffe „Überwachung", „Zertifizierung" und „Rezertifizierung" zu präzisieren und besser abzugrenzen. Das *LUKS* und die *SGMI* betrachten eine jährliche Überprüfung bei einem nur 3 Jahre gültigen Zertifikat als unverhältnismässig und fordern die Streichung von Absatz 1. Der *DSBAG* und die *privatim* schreiben wiederum, dass die jährliche Überprüfung aus datenschutzrechtlicher Sicht sehr zu begrüssen sei.

[66] BL, GL, LU, OW, UR, SH, SZ, ZG, TG, ZH, FR

HIN macht darauf aufmerksam, dass die umfangreiche Menge von Zertifizierungsanforderungen (Messpunkte) nur mit sehr grossem Aufwand geprüft werden könne. Entsprechend werde vorgeschlagen, die verschiedenen Kriterien nach MUSS und SOLL/KANN einzuteilen. Absatz 2 sei folgendermassen anzupassen: „Das BAG erstellt eine Liste aller Anforderungen und klassifiziert diese nach MUSS und SOLL-Kriterien. Wesentliche Abweichungen betreffen MUSS-Kriterien". Die *SQS* schreibt, dass das Register über die zertifizierten Stammgemeinschaften und Gemeinschaften durch das BAG geführt werde. Das BAG könne nach Artikel 36 Massnahmen ergreifen, wenn eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vorliegen würden. Ein zusätzlicher Absatz sei zu Artikel 33 hinzuzufügen: „ Das BAG kann von der Zertifizierungsstelle oder von der Gemeinschaft sowie der Stammgemeinschaft jederzeit die für die Zertifizierung oder Rezertifizierung relevanten Dokumente einfordern".

Art. 34 Geltungsdauer

Das Zertifikat wird für jeweils drei Jahre ausgestellt.

Die *BFH* und der Kanton *AG* wiederholen ihre Stellungnahmen von Artikel 33 Absatz 1 und die *FMH* ihren Kommentar von Artikel 28. Der *VAKA* schreibt, dass ihn das Misstrauen erstaune, welches den kommenden Gemeinschaften und Stammgemeinschaften entgegengebracht werde. Es sei vehement zu betonen, dass der Aufwand, alle 3 Jahre eine Zertifizierung anstehend zu haben definitiv nicht tragbar sei. Die *K3* und der *VZK* bezeichnen eine Rezertifizierung alle 3 Jahre ebenfalls als sehr aufwändig. Für die *Post* wäre eine Geltungsdauer von 5 Jahren adäquat, was Gemeinschaften betreffe. 3 Jahre würden für die IDM Sinn machen. Ähnlich wünschen 6 Kantone[67] folgende Umformulierung von Artikel 34: „[…] une durée de cinq ans". Insgesamt fordern 10 Stellungnehmende[68] die Ausstellung des Zertifikats für 5 Jahre.

Art. 35 Meldung wesentlicher technischer oder organisatorischer Anpassungen

[1] Gemeinschaften, Stammgemeinschaften und Herausgeber von Identifikationsmitteln müssen der Zertifizierungsstelle wesentliche technische oder organisatorische Anpassungen melden.

[2] Die Zertifizierungsstelle entscheidet, ob diese Anpassung durch eine Überwachung, eine Rezertifizierung oder eine ausserordentliche Rezertifizierung geprüft wird.

Der *VAKA* und die *Post* bitten um die Präzisierung des Begriffes „wesentlich". Der *VAKA* wünscht zudem die Nennung von Beispielen. *HIN* und die *BINT* weisen darauf hin, dass die Schwelle, was als „wesentlich" zu betrachten sei, recht hoch zu liegen habe, da die Zertifizierer ansonsten mit Meldungen überhäuft würden und verweisen auf den Hinweis von *HIN* zu Artikel 33. Der Kanton *AG* macht darauf aufmerksam, dass Anpassungen an IT-Infrastrukturen rasch zu aufwändigen Überprüfungen oder Rezertifizierungen führen können. Hier sei dem Prinzip der Verhältnismässigkeit Rechnung zu tragen.

Art. 36 Schutzklausel

Liegt eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vor, so kann das BAG:

a. Gemeinschaften und Stammgemeinschaften vorübergehend den Zugang zum elektronischen Patientendossier verweigern;
b. den Gebrauch bestimmter elektronischer Identifikationsmittel verbieten;
c. eine ausserordentliche Rezertifizierung anordnen.

Die *K3* und der *VZK* weisen darauf hin, dass aufgrund der unabsehbaren Folgen eines Ausschlusses einer Stammgemeinschaft oder einer Gemeinschaft, diese Möglichkeit nicht bestehen könne resp. dürfe. Wenn es möglich sei, eine Gemeinschaft auch nur vorübergehend vom elektronischen Patientendossier auszuschliessen, werde die Bedeutung, welche das elektronische Patientendossier gewinnen würde, völlig verkannt. Es müssten andere Mittel und Wege gefunden werden, um die Anforderungen an den Betrieb eines elektronischen Patientendossiers durchzusetzen. Es könne nicht sein, dass

[67] GE, FR, VS, VD, JU, NE

[68] VAKA, K3, VZK, Post, GE, FR, VS, VD, JU, NE

ein System abgestellt werde. Bspw. könnte eine Auffanggesellschaft die Aufgaben und Daten übernehmen. Die *FMH* schreibt, dass die Verfügbarkeit der Patientendaten ein zentraler Faktor für die Akzeptanz des elektronischen Patientendossiers sei. Sie schlagen für den Fall der Ausserbetriebnahme einer Gemeinschaft ebenfalls eine Art „Auffangeinrichtung" vor. Der Kanton *NW* sieht die Schutzklausel als problematisch an. Ein Ausschluss hätte zur Folge, dass bspw. Spitäler in einem Notfall keinen Zugriff auf notwendige Daten hätten. Damit würde die Patientensicherheit gefährdet, weshalb der Artikel zu überarbeiten sei. Der Kanton *SG* bittet um Klärung, welche Ansprüche Patientinnen / Patienten gegenüber wem geltend machen können, wenn das BAG vorübergehend den Zugang einer Gemeinschaft verweigere und die gespeicherten Patientendaten folglich nicht mehr verfügbar seien. 6 Kantone[69] machen geltend, dass das BAG einer Gemeinschaft nicht den Zugriff auf die elektronischen Patientendossiers verweigern könne, da die Gemeinschaft diese führe. Das BAG könne jedoch den Zugriff einer Gemeinschaft auf die zentralen Dienste und auf andere Gemeinschaften blockieren. Sie machen folgenden Formulierungsvorschlag für Buchstaben a: „[…] l'accès aux services centraux et aux autres communautés". Die *Tessaris* macht darauf aufmerksam, dass im Einzelfall neben der Zugangsverweigerung auch der Zugang unter besonderen Schutzmassnahmen zugelassen werden sollte, falls eine Gesundheitsfachperson den Zugang zum elektronischen Patientendossier aus Gründen der medizinischen Behandlung benötigt. Folgender Zusatz zu Buchstabe a wird vorgeschlagen: „[…] verweigern, wobei einer Gesundheitsfachperson zum Zweck einer medizinischen Behandlung im Einzelfall der Zugang zum elektronischen Patientendossier einer bestimmten Patientin oder eines Patienten unter Auferlegung besonderer Sicherheitsvorkehrungen gewährt werden kann". 6 Stellungnehmende[70] fordern die Überprüfung, ob eine „Kann-Vorschrift" hier tatsächlich zielführend sei. Wenn eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vorliege, solle das BAG handeln müssen. Der *DSBAG*, der *KDSBSON*, die *privatim* sowie die Kantone *BE* und *ZG* plädieren für folgende Formulierung von Artikel 36: „[…] des elektronischen Patientendossiers vor, nimmt das BAG insbesondere eine oder mehrere der folgenden Handlungen vor: a. verweigert den Gemeinschaften und Stammgemeinschaften vorübergehend den Zugang zum elektronischen Patientendossier; b. verbietet den Gebrauch bestimmter elektronischer IDM; c. ordnet eine ausserordentliche Rezertifizierung an".

3. Abschnitt: Sanktionen

Art. 37

[1] Die Zertifizierungsstelle kann die Gültigkeit eines Zertifikats aussetzen oder ein Zertifikat entziehen, namentlich wenn sie im Rahmen der Überwachung (Art. 33) schwere Mängel feststellt. Ein schwerer Mangel liegt insbesondere vor, wenn:

a. wesentliche Voraussetzungen der Zertifizierung nicht mehr erfüllt sind; oder
b. ein Zertifikat in irreführender oder missbräuchlicher Art und Weise verwendet wird.

[2] Bei Streitigkeiten über die Sistierung oder den Entzug richten sich die Beurteilung und das Verfahren nach den zivilrechtlichen Bestimmungen, die anwendbar sind auf das Vertragsverhältnis zwischen Zertifizierungsstelle und zertifizierter Gemeinschaft oder Stammgemeinschaft oder zertifiziertem Herausgeber von Identifikationsmitteln.

[3] Besteht der begründete Verdacht, dass eine zertifizierte Gemeinschaft oder Stammgemeinschaft oder ein zertifizierter Herausgeber von Identifikationsmitteln die Zertifizierungsvoraussetzungen nicht einhält, so kann das BAG:

a. eine Überprüfung durch die Zertifizierungsstelle anordnen;
b. die Gültigkeit des Zertifikats aussetzen;
c. das Zertifikat entziehen.

Der Kanton *SG* wiederholt seine Stellungnahme von Artikel 36. Der *VAKA* weist darauf hin, dass im Falle eines Entzugs des Zertifikats einer Gemeinschaft oder auch ein „temporäres vom Netz nehmen" einer Gemeinschaft im Sinne der Patientinnen / Patienten heute keine Regelung über Auffanggemeinschaften bzw. deren Gesellschaften bestehe. Die Definition des Verfahrens, Organisation und Management einer „Auffanggesellschaft" sei vollständig zu überdenken und definieren. Die *RPB* fügt an, dass ein abgeschwächtes Szenario aus Artikel 8 denkbar sei. Die *SQS* wünscht, dass in Artikel 37 ein zusätzlicher Absatz eingefügt werde, der die Folgen einer Sistierung oder eines Entzugs der Zertifizierung

69 FR, NE, GE, VS, VD, JU
70 DSBAG, KDSBSON, privatim, AG, BE, ZG

regelt, um die Interessen der betroffenen Leistungserbringer und Patientinnen / Patienten auf Zugang zum elektronischen Patientendossier zu schützen.

Bezüglich des ersten Absatzes bezeichnen 7 Stellungnehmende[71] eine „Kann-Vorschrift" beim Vorliegen schwerer Mängel als nicht angemessen. Vielmehr gelte es die Zertifizierungsstelle beim Vorliegen schwerer Mängel zu verpflichten, die Gültigkeit des Zertifikats auszusetzen oder das Zertifikat zu entziehen. Der Absatz sei entsprechend anzupassen. Im Rahmen des zweiten Absatzes machen die *GDK* sowie 11 Kantone[72] darauf aufmerksam, dass das Rechtsverhältnis zwischen der akkreditierten Stelle und interessierten Unternehmen unsicher sei. Erstere erfülle Verwaltungsaufgaben, was Fragen nach staatlicher Kontrolle, Rechtsschutz und Grundrechtsbindung aufwerfe. Die aufgestellte Behauptung, das Verfahren richte sich nach den zivilrechtlichen Bestimmungen, die „anwendbar sind auf das Vertragsverhältnis", dürfte daher in dieser Absolutheit nicht zutreffen. Absatz 2 sei dementsprechend zu überarbeiten. Im Zuge des dritten Absatzes schreiben der *DSBAG*, die *privatim* sowie die Kantone *AG*, *BE* und *FR*, dass das Verwaltungsverfahren zur Anwendung komme, da das BAG die Entscheidungsbehörde sei (Art. 1 VwVG, SR 172.021). In diesem Zusammenhang solle geprüft werden, ob das Verwaltungsverfahren hier die notwendigen Handlungsfreiheiten bezüglich Schnelligkeit, Effektivität usw. zu gewährleisten vermöge. Die *SQS* weist darauf hin, dass das EPDG das BAG nicht berechtige, aktiv in den konkreten Zertifizierungsprozess einzugreifen und die Rolle der Zertifizierungsstelle zu übernehmen. Die Ermächtigung des BAG gemäss Artikel 37 Absatz 3 verletze das Legalitätsprinzip und sei nicht mit einer Ausführungsverordnung in Einklang zu bringen. Zudem könne das BAG bei Fällen, in denen rasch gehandelt werden müsse, nach Artikel 36 Massnahmen ergreifen. Artikel 37 Absatz 3 Buchstaben b und c seien ersatzlos zu streichen.

3.1.7 7. Kapitel: Abfragedienste

1. Abschnitt: Allgemeines

Art. 38

[1] Die Abfragedienste enthalten:

a. die Referenzdaten über:
   1. die Gemeinschaften und Stammgemeinschaften,
   2. die Gesundheitseinrichtungen und deren Gesundheitsfachpersonen, die Daten des elektronischen Patientendossiers bearbeiten dürfen;
b. die Metadaten (Art. 9 Abs. 3 Bst. b);
c. die Austauschformate (Art. 9 Abs. 3 Bst. c);
d. die für das elektronische Patientendossier registrierten Objektidentifikatoren (OID).

[2] Das BAG stellt den Aufbau, den Betrieb und die Weiterentwicklung der Abfragedienste sicher.

Die *K3* und der *VZK* schreiben, dass die Abfragedienste nach Artikel 38 ff. verschiedene nützliche Daten für die Kommunikation zwischen Gesundheitsfachpersonen und Gesundheitseinrichtung enthielten. Sie fragen, ob diese Register auch für die gerichtete Kommunikation genutzt werden könne. Im Kanton Zürich sei eine Nutzung der Infrastruktur auch für die primäre Kommunikation zwischen 2 Leistungserbringern vorgesehen. Sie bitten daher um die Ermöglichung der Nutzung des MPI für die gerichtete Kommunikation zwischen Leistungserbringern. Die *OFAC* schreibt, dass sie, aufgrund ihrer grossen Erfahrung im IT-Betrieb dieses Dienstleistungstyps auf nationaler Ebene und aufgrund der Kritikalität in Bezug auf die Verfügbarkeit, die Sicherheit und den Datenschutz, usw. empfiehlt, dass die Gemeinschaften, die diese zentralen Dienstleistungen anbieten werden, auch zertifiziert sein sollen (z.B. ISO20000, ISO27001, OCPD). Die Organisationen, die die Dienstleistungen verwalten und betreiben werden, werden mindestens den gleichen Zertifizierungs- und Organisationsanforderungen unterworfen. Gemäss der *OFAC* sollte dies in der EPDV vorgeschrieben werden und es müsse sich zudem in den Anforderungen zum Ausschreibungsverfahren befinden.

[71] DSBAG, KDSBSON, privatim, AG, BE, FR, ZG
[72] BL, GL, LU, OW, UR, NW, FR, SZ, TG, ZG, ZH

2. Abschnitt: Inhalt

Art. 39 Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften

[1] Der Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften enthält folgende Daten:

a. ihre Bezeichnung;
b. ihre GLN;
c. ihre OID;
d. ihre Zertifikate zur sicheren Authentifizierung gegenüber anderen Gemeinschaften und Stammgemeinschaften;
e. die Internetadresse ihres Zugangspunktes.

[2] Das BAG prüft diese Daten und trägt sie im Abfragedienst der Gemeinschaften und Stammgemeinschaften ein.

Die *Post* kritisiert, dass der Begriff „Zertifikat" missverständlich sei und „Authentifizierungszertifikat" zu bevorzugen wäre.

Art. 40 Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen

Gemeinschaften und Stammgemeinschaften tragen im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen folgende Daten ein:

a. zu Gesundheitseinrichtungen und Gruppen von Gesundheitsfachpersonen:
    1. die Bezeichnung und die Adresse,
    2. die GLN,
    3. die OID;
b. zu Gesundheitsfachpersonen:
    1. die Personalien,
    2. die GLN,
    3. die Bezeichnung und die Adresse der Gesundheitseinrichtung oder der Gruppe von Gesundheitsfachpersonen, der sie angehört.

PH CH wiederholt an dieser Stelle ihre Bemerkungen zu Artikel 8. Der *VAKA* fragt, ob es Use Cases gebe, in welchen es passieren könne, dass mehrere Gemeinschaften gleiche Einträge von HPD unterschiedlich anpassen würden. Gesundheitsfachpersonen seien durchaus in mehreren Gemeinschaften und mit vielen verschiedenen Organisationszugehörigkeiten aktiv. Es solle sichergestellt werden, dass keine solchen Überschneidungen entstehen. *H+* begrüsst ausdrücklich den Ansatz, dass das BAG hier einen nationalen Abfragedienst für die Umsetzung festlegt. Die *Post* schreibt, dass der Begriff „Gesundheitseinrichtung" hier zum ersten Mal eingeführt werde. In den Kapiteln zur Autorisierung sei nur „Gruppen" benutzt worden. Es stelle sich die Frage, ob eine Gesundheitseinrichtung auch eine Gruppe sein könne. Die Begrifflichkeiten seien klar zu definieren und es sollte ersichtlich sein, ob Gruppen im Abfragedienst verwaltet werden oder nicht. Zudem sei unklar und zu klären was passiere, wenn zwei Gemeinschaften dieselben Einträge ändern wollen und wer in einem solchen Fall die Verantwortung übernehmen würde. Bezüglich Buchstabe a Ziffer 3 fragt die *Post* des Weiteren, ob es das Ziel der Verordnung sei, dass sich jede Gesundheitseinrichtung in der Schweiz neben der GLN neu auch noch eine OID beschaffen muss. Gruppen würden im Folgenden so beschrieben, dass sie sowohl global als auch individuell sein können. Diese Entscheidung werde den Patientinnen / Patienten überlassen. Ein eindeutiger Identifier mache in diesem Use Case Szenario keinen Sinn, weil die gleiche Gruppe je nach Kontext andere Mitglieder habe. Die GLN genüge als Identifier. Der Sachverhalt sei zu klären und die Formulierung von Ziffer 3 solle folgendermassen angepasst werden: „OID als eindeutiger Identifier innerhalb der OID der Gemeinschaft".

Buchstabe b: Die *HL7* und *IHE* schreiben bezüglich den Ziffern 1 und 3, dass die verlangten Personalien abschliessend aufzuführen seien. Ziffer 3 könne folgendermassen formuliert werden: „die GLN und falls vorhanden die OID, sowie die Bezeichnung […]". Die *Post* stellt an dieser Stelle fest, dass die Gesundheitsfachpersonen gemäss Buchstabe a Ziffer 2 die GLN einer bereits erfassten Gruppe oder Organisation anzugeben habe. Diese Angaben seien bereits unter Buchstabe a Ziffer 1 zu machen. Die *ASPS* und der *Spitex* machen darauf aufmerksam, dass die Vergabe von GLN-Nummern an Pflegefachpersonen erst am Entstehen und weit von einer Vollständigkeit entfernt sei. Es sei die Verbindlichkeit zu schaffen, dass an jede Pflegefachperson eine GLN vergeben werde.

3. Abschnitt: Übertragung an Dritte

Art. 41 Leistungsvertrag

[1] Das BAG kann den Aufbau und den Betrieb der Abfragedienste mittels Leistungsvertrag an Dritte übertragen.

[2] Der Leistungsvertrag regelt insbesondere:

a. die zu erreichenden Ziele;
b. die Anforderungen an den Datenschutz und die Datensicherheit;
c. den Umfang und die Modalitäten der Entschädigung durch den Bund;
d. die Folgen einer Nichterfüllung;
e. die Modalitäten für eine periodische Berichterstattung.

[3] Der beauftragte Dritte ist verpflichtet, das BAG umgehend über wesentliche Änderungen zu informieren.

Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* schreiben, dass nicht geregelt sei, nach welchen Kriterien die Höhe der Entschädigung an den Dritten bestimmt werde. Es müsse aber aufgrund von Artikel 42 damit gerechnet werden, dass diese Kosten des Dritten auf die Gemeinschaften bzw. Stammgemeinschaften überwälzt werden. Damit sich die Kosten in einem vernünftigen Rahmen bewegen, dürfe die Entschädigung an den Dritten nicht nach privatwirtschaftlichen Kriterien ausgehandelt bzw. festgelegt werden. Das Äquivalenzprinzip sei zu beachten. Sie fordern folgenden zusätzlichen Absatz: „Die Entschädigung des Dritten, bestehend aus allfälligen Gebühren für die Erbringung von Leistungen gemäss Artikel 19 Absatz 2 EPDG sowie einer zusätzlichen Entschädigung des Bundes, darf den Aufwand, welcher anfiele, wenn das BAG den Aufbau und den Betrieb der Abfragedienste selber vornehmen würde, nicht übersteigen." Die *KAeG SG* wünscht zudem folgenden zusätzlichen Satz am Ende des neuen Absatzes: „Eine Beteiligung durch die Ärzteschaft ist ausgeschlossen".

Art. 42 Gebühren

[1] Von den Gemeinschaften und Stammgemeinschaften wird pauschal eine jährliche Gebühr von 13 500 Franken erhoben.

[2] Im Übrigen gelten die Bestimmungen der Allgemeinen Gebührenverordnung vom 8. September 2004.

Die *FMH* wiederholt ihren Kommentar von Artikel 28 und Artikel 34. 20 Stellungnehmende[73] weisen darauf hin, dass Absatz 1 eine jährliche Gebühr über CHF 13'500 enthalte, während die Erläuterungen von einer Gebühr über CHF 20'000 sprechen. Das *KSOW* fragt, wie die CHF 13'500 zustande kommen oder ob es doch CHF 20'000 seien. Gemäss dem *VGIch* und der *Medgate* sei dieser Widerspruch aufzuheben. Der Kanton *BE* beantragt, dass die Restriktionen bei den TOZ für Gemeinschaften und Stammgemeinschaften präzisiert werden. 17 Stellungnehmende[74] machen geltend, dass es sachwidrig sei, einerseits den Aufbau von Gemeinschaften durch Finanzhilfen zu unterstützen und andererseits die Betriebskosten der Gemeinschaften durch eine Gebühr zu erhöhen, womit ein Teil der Finanzhilfen wieder zurückverlangt werde. Ähnlich bezeichnen 9 weitere Stellungnehmende[75] eine jährliche Gebühr, unter Berücksichtigung der Finanzhilfen des Bundes, als sinnlos. Das *LUKS* und die *STSAG* verweisen ebenfalls auf die Finanzhilfe und darauf, dass auf eine Gebühr zu verzichten sei. Die *BRH* ist der Ansicht, dass die jährliche Gebühr für den Aufbau und Betrieb der Abfragedienste über 10 Jahre in Frage zu stellen sei, da ein Teil der Finanzhilfe vom Bund wieder zurückfliesse. Sie schlägt eine Verrechnung mit der geleisteten Finanzhilfe vor und fordert die Korrektur des Gebührenbetrages. Das *LUKS* schreibt zudem, dass der Bund die zentralen Abfragedienste finanzieren solle und die *STSAG* verweist darauf, dass das EPDG einen Zwang zur Teilnahme für Institutionen vorsehe, womit nicht auch nicht ein Zwang zur Finanzierung verbunden werden könne. Die Kantone *NW*, *ZG* und *ZH* sowie der *ZAD* sind der Meinung, dass es keinen Grund für diese Gebühr gebe. Ihre Unzulässigkeit ergebe sich auch daraus, dass sich aus der Verordnung nicht ergebe, welche Leistung mit dieser Gebühr abgegolten werden solle. Auch aus den Erläuterungen lasse sich diesbezüglich nichts entnehmen. Gemäss 6 Kantonen[76] müsse der Bund die operativen Kosten im allgemeinen Interesse übernehmen, insbesondere für den Betrieb

[73] GDK, BL, GL, LU, OW, UR, SH, AR, ZG, SZ, AI, TG, PKS, BE, BFH, SVP, BRH, VGIch, Medgate, LUKS
[74] GDK, BL, GL, LU, OW, UR, SH, AR, ZG, SZ, AI, TG, PKS, NW, ZH, ZG, ZAD
[75] FR, NE, GE, VS, VD, JU, K3, VZK, SVP
[76] FR, NE, GE, VS, VD, JU

der zentralen Dienste. Ähnlich spricht sich die *OFAC* dafür aus, dass der Bund und nicht die Gemeinschaft diese Kosten vollständig übernehmen solle. Für den Kanton *AR* sei insbesondere zu klären, welche Kosten mit dieser Gebühr gedeckt werden sollen und an wen die Gelder fliessen würden. Der *VAKA* ist der Meinung, dass es in einer Situation, in welcher keine einzige, zukünftige Gemeinschaft ein Geschäftsmodell für die Finanzierung des Betriebes kenne, keine Gebühren für zentrale Dienste erhoben werden sollten. Die *SVP* weist darauf hin, dass es sowohl im Interesse der Gemeinschaften als auch der Behörden wäre, wenn die Finanzflüsse vereinfacht würden, z.B. indem die Höhe der Finanzhilfen so festgelegt werde, dass auf Gebühren verzichtet werden könne.

Insgesamt fordern 25 Stellungnehmende[77] explizit die Streichung von Artikel 42. *HIN* gehe davon aus, dass sich sehr unterschiedliche Gemeinschaften bilden werden. Sie schlägt vor, dass die Gebühren grössenabhängig erhoben werden und formuliert folgenden Text für Artikel 42 Absatz 1: „[…] wird pauschal eine grössenabhängige, jährliche Gebühr von maximal CHF 13‘500 erhoben“. Die *BFH* schreibt, dass auch hier allenfalls mit einem Sockelbetrag und einem variablen Teil, wie. z.B. Anzahl Bürgerinnen / Bürger in der Gemeinschaft, etwas mehr ausgleichende Gewichtung vorzusehen, dies insbesondere für die Stammgemeinschaften. Starr genannte Beträge würden wenig sinnvoll erscheinen.

Art. 43 Aufsicht

[1] Das BAG ist zuständig für die Aufsicht über Dritte, denen der Betrieb eines Abfragedienstes übertragen ist.

[2] Die Aufsicht umfasst insbesondere:

a. die periodische Prüfung, ob die Vorgaben nach Artikel 41 Absatz 2 eingehalten werden;
b. die periodische Einforderung von Berichten;
c. die Kontrolle der Einhaltung des Leistungsvertrags vor Ort.

Die *SGMI* weist an dieser Stelle darauf hin, dass die Gebühren im 3. Abschnitt: „Übertragung an Dritte“ aufgeführt seien. Dies müsse präzisiert werden, Gebühren würden wohl generell gelten.

[77] VAKA, FR, NE, GE, VS, VD, JU, K3, VZK, FMH, BL, GDK, GL, LU, OW, UR, SH, SZ, AR, AI, TG, ZG, NW, ZH, ZAD

3.2 EPDV-EDI

Im Rahmen der EPDV-EDI sind die Anhänge 5b, 5c und 8 in englischer Sprache verfasst. Die Stellungnahmen zu diesen drei Dokumenten sind dementsprechend ebenfalls vorwiegend in Englisch eingereicht worden und wurden ohne Übersetzung in diesen Bericht integriert.

3.2.1 Art. 1 Patientenidentifikationsnummer (Anhang 1)

Art. 1	Patientenidentifikationsnummer
Der Aufbau der Patientenidentifikationsnummer und das Vorgehen zur Kontrollzifferprüfung bei der manuellen Erfassung der Patientenidentifikationsnummer nach Artikel 4 Absatz 2 EPDV sind in Anhang 1 festgelegt.	

Artikel 1: Der Kanton *FR* weist darauf hin, dass es nötig sei zu klären, was mit der PID möglich ist resp. gemacht werden kann und was nicht.

Anhang 1

Die *Stiftung refdata*, *GS1*, die *SGMI* und *ICTS* wiederholen bezüglich des Anhanges 1 ihre Stellungnahmen von Artikel 4 EPDV. *ICTS* fordert ausserdem, dass punkto Patientenidentifikation und den dafür verwendeten Identifikationsschlüsseln die Umsetzung des Grundsatzes, dass internationale Standards zum Zuge kommen sollen und auf isolierte schweizerische Eigenentwicklungen, wo immer möglich, zu verzichtet sei. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* begrüssen, dass eine eigens für das elektronische Patientendossier bestimmte PID geschaffen wird und nicht, wie ursprünglich beabsichtigt, die AHVN13 als Identifikationsnummer verwendet.

Die *OFAC* schreibt, dass hinsichtlich des Regelalgorithmus nichts zu erklären sei. Die *BINT*, die *HL7* und *IHE* bezeichnen das Verfahren als üblich, es entspreche einem Standard und genüge den Anforderungen aus ihrer Sicht. Aus Sicht der *medshare* ist Anhang 1 ebenfalls in Ordnung.

3.2.2 Art. 2 Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (Anhang 2)

Art. 2	Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften
Die technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ) für Gemeinschaften und Stammgemeinschaften nach Artikel 29 Absatz 2 EPDV sind in Anhang 2 festgelegt.	

Artikel 2: Die *SQS* macht geltend, dass der Anhang 2 keine „Zertifizierungsvoraussetzung“ sei, sondern eine „technische und organisatorische Vorgabe an Gemeinschaften und Stammgemeinschaften“, die nach Artikel 11 Absatz 1 Buchstabe a EPDG der Zertifizierungspflicht unterstehe und zertifiziert werden müsse. Es sei nicht Sache einer Zertifizierung von Managementsystemen die korrekte Einhaltung von technischen Vorgaben zu überprüfen. Im Rahmen einer ISO/IEC 27001:2013 Zertifizierung müsse das Auditorenteam via Control A.18 die Anwendung innerhalb der Managementsystemzertifizierung prüfen. Aus diesem Grund solle Artikel 2 folgendermassen lauten: „Die technischen und organisatorischen Voraussetzungen (TOV) für Gemeinschaften und Stammgemeinschaften, die der Zertifizierungspflicht nach Artikel 11 Absatz 1 EPDG unterstehen, sind gemäss Artikel 29 Absatz 2 EPDV in Anhang 2 festgelegt“. Zudem fordert die *SQS* folgenden, zusätzlichen Absatz in Artikel 2: „Die Mindestanforderungen an ein Datenschutzmanagementsystem richten sich nach Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 19. März 2014 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten“.

Anhang 2

1. Verwaltung (Art. 8 EPDV)

6 Stellungnehmende[78] bezeichnen die Vorgaben in Ziffer 1 als zu umfangreich und seien dementsprechend zu vereinfachen. Die meisten dieser Vorgaben würden sich bereits aus Artikel 8 EPDV ergeben. Diejenigen Vorgaben, die darüber hinausgehen, sollten dort als generell-abstrakte Regelungen aufgenommen werden (Beispiel: Ziffer 1.3 über die Verwaltung von Hilfspersonen)

1.1 Verwaltung von Gesundheitseinrichtungen (Bst. a und c):

6 Kantone[79] weisen darauf hin, dass das Wort „gestion" in der französischen Übersetzung nicht angemessen sei. Es müsse mit „Administration" (was die Übersetzung von „Verwaltung" sei) ersetzt werden.

1.1.1: Die *IG eHealth* und die *Post* wünschen, dass der Begriff der Gesundheitseinrichtung definiert wird. Insbesondere sei zu klären, ob ein niedergelassener Arzt, ein Therapeut oder eine Hebamme grundsätzlich nur als "Mitarbeiter" einer Gesundheitseinrichtung in einer Gemeinschaft teilnehmen könne. Ähnlich bemängelt die *Tessaris*, dass der Begriff „Gesundheitseinrichtung", der in Artikel 8 Absatz 1 EPDV eingeführt worden sei, nirgends klar definiert wurde.

1.1.2: Die *FMH* schreibt bezüglich Ziffer 1.1.2.1, dass das EPDG nicht die Prozesse in der Arztpraxis, Spital, etc. regle. Hier könne nur etwas in Bezug auf die Nutzung des elektronischen Patientendossiers geregelt werden. Die *IG eHealth* und die *Post* geben zu bedenken, dass die Anforderung gemäss Ziffer 1.1.2.2 nur erfüllt werden könne, wenn die Dienste die entsprechenden Prozesse und technischen Mittel zur Verfügung stellen. Diese Anforderungen seien nirgends beschrieben. Sie schlagen somit vor, dass verpflichtende Anforderungen an die Dienste gemäss Artikel 40 in der Verordnung (oder Anhängen) formuliert werden müssen.

Die *GDK* und 10 Kantone[80] schreiben bezüglich Ziffer 1.1.2.3, dass die Formulierung „für alle mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen" suggerieren könnte, dass ausnahmslos jede Gesundheitsfachperson einer Gesundheitseinrichtung ins HPD aufgenommen werden müsse. Es müsse den Gesundheitseinrichtungen frei stehen, die Selektion der Gesundheitsfachpersonen auf jene zu beschränken, die das elektronische Patientendossier nutzen werden. Ziffer 1.1.2.3 solle dementsprechend neu folgendermassen lauten: „der Prozess „Eintritt von Gesundheitsfachpersonen" für jene mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen ausgelöst wird, welche die Gesundheitseinrichtung für den Zugriff aufs elektronische Patientendossier vorsieht". Betreffend dieser Ziffer schreibt der *VGIch*, dass es gemäss den Erläuterungen möglich sei, dass den Gesundheitseinrichtungen der Eintrittsprozess delegiert werden könne. Die Bestimmung müsse aus Praktikabilitätsgründen dahingehend interpretiert werden, dass die Gesundheitseinrichtung selbst bezeichnen kann, wer aktiv eintritt. Die hohe Fluktuation in den Spitälern fordere einen vernünftigen Umgang mit dieser Anforderung. Die TOZ sei dahingehend anzupassen. Der Kanton *AR* plädiert dafür, dass die Darstellungen unter der Ziffer 1.1.2.3 in die Verordnungen etabliert werden. Die *Post* fragt, wie eine Gesundheitsfachperson eintreten könne, wenn die Gesundheitseinrichtung nicht Mitglied der Gemeinschaft sei. Es müsse klarer formuliert werden was gemeint ist. Gemäss dem *KSSG* beschreibt Ziffer 1.1.2.3, dass über alle eintretenden Gesundheitsfachpersonen informiert werden müsse, was ein Widerspruch zu den gemachten Aussagen in den Informationsveranstaltungen darstelle. Dort sei mehrfach gesagt worden, dass nur einige Gesundheitsfachpersonen je Fachbereich/Klinik berechtigt und aufgelistet werden müssen. Der Artikel sei entsprechend zu konkretisieren.

1.1.3: Die *SUVA* macht geltend, dass die Ablage der Dokumente in einer Gesundheitseinrichtung der

[78] K3, VZK, ZAD, ZH, ZG, NW
[79] FR, NE, GE, VS, VD, JU
[80] BL, GL, LU, OW, UR, BS, NW, FR, SZ, TG

Ablage im Primärsystem entspreche. Mit der Pflicht der Dokumentenlöschung in den Dokumentenablagen der Gesundheitseinrichtung gingen die Dokumente endgültig verloren. Dies könne nicht Sinn und Zweck des elektronischen Patientendossiers sein. Unabhängig von einer Löschung des elektronischen Patientendossiers oder dem Austritt einer Einrichtung aus einer Gemeinschaft müssen die Dokumente in den Primärsystemen weiterhin vorhanden sein. Die Löschungspflicht sei zu streichen resp. wird die ersatzlose Streichung von 1.1.3 inkl. 1.1.3.1 bis 1.1.3.2.3, oder zumindest eine Präzisierung gefordert. Die *Post* schreibt bezüglich Ziffer 1.1.3.1, dass diese Anforderung nicht erfüllbar sei, wenn ein Leistungserbringer in mehreren Einrichtungen arbeitet oder in mehreren Gemeinschaften definiert wird. Wenn z.B. ein Arzt eine Praxis in Nyon hat und Belegarzt in Genf ist, wäre er in zwei HPD registriert. Es gebe Ärzte bei der *SUVA*, welche in bis zu 7 Einrichtungen arbeiten. Die Formulierung sei dementsprechend zu ändern. Gemäss dem Kanton *TI* sollte bezüglich den Bestimmungen unter 1.1.3.2 berücksichtigt werden, dass die Daten von einer Gesundheitsfachperson eingegeben werden, um der Patientin / dem Patienten eine Weiterführung der optimalen Behandlung zu gewährleisten. Die Daten gehören somit nicht der Einrichtung, die aus der Gemeinschaft austritt, sondern sind Eigentum der Patientin / des Patienten. Sie sollten folglich nie gelöscht, sondern allenfalls migriert werden, um ihr / ihm ein möglichst umfassendes Dossier zu gewährleisten. Auf jeden Fall dürfe die allfällige Löschung nicht erfolgen, ohne dass sie / er vorgängig informiert wurde. Die *SGMI* machen geltend, dass betroffene Patientinnen / Patienten bei dem Austritt einer Gemeinschaft die Möglichkeit haben müssen, sich einer anderen Gemeinschaft anzuschliessen. Dies sei zu präzisieren. Nach der Meinung der *FMH* könne es nicht sein, dass in den meisten kantonalen Gesetzgebungen geregelt werde, wie die Patientendaten bspw. beim Tod eines Praxisinhabers den Patientinnen / Patienten zur Verfügung gestellt werden müssen, beim elektronischen Patientendossier hingegen die Daten gelöscht werden resp. die weitere Aufbewahrung der Patientin / dem Patienten überantwortet wird (s. 1.1.3.2.3) und das Vorgehen durch die jeweilige Gemeinschaft selbst festgelegt wird. Es sei entgegen den Interessen der Patientin / des Patienten und entgegen den Grundregeln der medizinischen Dokumentation. Es könne auch nicht sein, dass eine Anforderung von solcher Tragweite einzig ein Zertifizierungskriterium in den TOZ ist, und nicht als funktionale Anforderung auf Ebene Verordnung definiert werde. Es seien entsprechende Massnahmen zu treffen.

6 Kantone[81] machen geltend, dass im Falle eines Austrittes einer Gesundheitseinrichtung nach den Ziffern 1.1.3.2.1 und 1.1.3.2.2 die elektronischen Patientendossiers nicht gelöscht werden dürfen. Sie müssen den Patientinnen / Patienten und den Gesundheitsfachpersonen weiterhin zur Verfügung stehen. Zudem sind nicht die Einrichtungen die Autoren der Dokumente, sondern die Gesundheitsfachpersonen. Die beiden Ziffern seien dementsprechend zu streichen. Für die *BFH* ist es unverständlich, wenn die Dokumente einer austretenden Gesundheitseinrichtung einfach gelöscht werden. Auch wenn die Patientinnen / Patienten gemäss 1.1.3.2.3 rechtzeitig informiert werden müssen, sollte es einen klaren Prozess geben, der den Verlust der Dokumente verhindere. Ziffer 1.1.3.2.3 sollte dahingehend erweitert werden, dass die „zu löschenden" Dokumente mindestens automatisiert in die nach Artikel 18 EPDV „dedizierte gemeinschaftsinterne Dokumentenablagen" der betroffenen Patientinnen / Patienten übertragen werden. *Economiesuisse* und *SBC* machen darauf aufmerksam, dass die Patientin / der Patient in keinem Fall die Daten verlieren dürfe, wenn eine Gesundheitseinrichtung aus dem EPDG Vertrauensraum austritt. Dies wäre im Sinne der Patientensouveränität nicht opportun. Es wird die Aufnahme des folgenden Textes vorgeschlagen: „Die Gemeinschaften müssen sich organisieren für die weitere Speicherung von Dokumenten von Leistungserbringern, die die Gemeinschaft verlassen und die zu keiner anderen Gemeinschaft gehen". *Bleuer* weist darauf hin, dass die Dokumente der Patientin / dem Patienten gehören und ohne ihre / seine explizite Einwilligung nichts gelöscht werden dürfe. Es sei in geeigneter Weise dafür zu sorgen, dass alle Dokumente der austretenden Gesundheitseinrichtung im elektronischen Patientendossier erhalten bleiben (aus Sicht der Benutzer dürfe sich betreffend Zugriff nichts ändern). Ähnlich schreibt die *medshare*, dass ein elektronisches Patientendossier von der Eröffnung bis zum Tod der Patientin / dem Patienten gehöre. Aus diesem Grund habe niemand ausser ihr / ihm das Recht Daten zu löschen. Selbst bei einer Aufhebung müsse sie / er das Recht haben zu entscheiden, ob die Daten gelöscht werden sollen oder nicht. Diese Frage sei insbesondere im Falle einer späteren Wiedereröffnung von zentraler Bedeutung. Gemäss der *IG eHealth* und der *Post* ist Ziffer

[81] FR, NE, GE, VS, VD, JU

1.1.3.2.1 nicht nachvollziehbar. Trete eine Gesundheitseinrichtung aus einer Gemeinschaft aus, dann sei es Sache der neuen Gemeinschaft, die Gesundheitseinrichtung wieder korrekt zu erfassen. Die Identifikatoren von Gesundheitseinrichtung und Gesundheitsfachpersonen (GLN) blieben erhalten. Die Verknüpfung mit Dokumenten auch. Wichtig sei, dass eine Gesundheitseinrichtung ihre Dokumente nicht in eine neue Gemeinschaft mitnehmen kann, da die Verknüpfung der Dokumente ändere, wenn sich die ID der Affinity Domain ändere. Alle Referenzen in den Audit Logs würden verloren gehen. Damit wäre auch 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. Die Anforderung sei dementsprechend zu streichen. Die *IG eHealth* und die *Post* sprechen sich ausserdem dafür aus, dass die elektronischen Patientendossiers beim Austritt einer Gesundheitseinrichtung nicht zu deren Löschung führen dürfe. Die *IG eHealth* schlägt vor, dass die ausscheidende Gesundheitseinrichtung die Daten im Repository lassen müsse, welches dann in den Besitz der Gemeinschaft übergehe. Die *Post* fügt an, dass die Forderung der Löschung nach Ziffer 1.1.3.2.1 mit dem Zweck des Gesetzes nicht vereinbar sei. Es widerspreche dem Prinzip der sekundären Datenhaltung sowie der Grundidee, dass die Datenhoheit bei den Patientinnen / Patienten liegt. Die Gemeinschaft müsse sicherstellen, dass alle Dokumente auch nach dem Austritt einer Gesundheitsfachperson oder einer Gesundheitseinrichtung weiterhin verfügbar sind. Für die *Integic* ist die Formulierung in Ziffer 1.1.3.2.1 nicht verständlich; die Wahrnehmung der Patientin / des Patienten sei, dass sich die ihn betreffenden Dokumente in seiner (einer) Ablage befinden. Wie auch immer das Konstrukt sei, offenbar gehen der Patientin / dem Patienten im Anwendungsfall nach 1.1.3 und 1.1.3.2 Daten verloren; sonst müsste sie / er nicht gemäss 1.1.3.2.3 benachrichtigt werden. Medizinische Dokumente gehören der Patientin / dem Patienten. Eine Löschung durch Dritte – aus was für Gründen auch immer – sei wohl nicht rechtens. Eine explizite Formulierung eines Modells zur Datenherrschaft werde nicht formuliert; Formulierungen wie in 1.1.3.2.1 und 1.1.3.2.2 liessen vermuten, dass zumindest implizit von Verfügungsrechten Dritter betreffend Aufbewahrung ausgegangen wird. Ziffer 1.1.3.2.1 sei nur dann zutreffend, wenn die Ablage für das elektronische Patientendossier exklusiv ist. In den Erläuterungen zum EPDV werde von Ausnahmefällen gesprochen, hier nicht. Die *privatim* gibt zu bedenken, dass die blosse Löschung von Dokumenten nicht für deren Vernichtung ausreiche. Die Daten seien vielmehr durch geeignete technische Verfahren unwiderruflich zu zerstören. Sie machen folgenden Formulierungsvorschlag für Ziffer 1.1.3.2.1: „[…] austretenden Gesundheitseinrichtung durch geeignete technische Massnahmen unwiderruflich vernichtet werden“. Für Ziffer 1.1.3.2.2 schlagen sie folgenden Wortlaut vor: „[…] austretenden Einrichtung verweisen durch geeignete technische Massnahmen unwiderruflich vernichtet werden“. Die Kantone *LU*, *NW*, *SZ* und *ZH* bezeichnen es als problematisch, dass die Dokumente, die eine austretende Gesundheitseinrichtung im elektronischen Patientendossier erfasst hat, gelöscht werden sollen, wenn sie aus der Gemeinschaft austritt. Es sei zu klären, ob die Patientin / der Patient oder die Gesundheitseinrichtung die Herrschaft über diese Dokumente habe. Gegen den Willen der Patientin / des Patienten dürfen keine Daten aus dem elektronischen Patientendossier gelöscht werden. Der Kanton *ZG* schreibt, dass der Austritt einer Gesundheitseinrichtung nicht zur Löschung von Daten im elektronischen Patientendossier führen dürfe und dies unabhängig davon, ob die Einrichtung einer anderen Gemeinschaft beitrete oder nicht. Es sei eine Regelung aufzunehmen, die sicherstellt, dass die Daten der Patientinnen / Patienten im elektronischen Patientendossier bleiben, auch wenn die Gesundheitseinrichtung, welche die Daten eingestellt hat, aus der Gemeinschaft oder Stammgemeinschaft austritt. Die *Tessaris* macht darauf aufmerksam, dass das zuverlässige Löschen eines Dokumentes im elektronischen Patientendossier, einschliesslich der vorhandenen Back-up Kopien, eine aufwändige Angelegenheit sei. Es stelle sich die Frage, ob die Gemeinschaft oder die Gesundheitseinrichtung dafür verantwortlich sei und die Kosten trage. Die Ziffer 1.1.3.2.1 solle folgendermassen angepasst werden: „[…] Gesundheitseinrichtung, einschliesslich Sicherungs- und Back-up Kopien, vollständig gelöscht werden und der Vollzug der Löschung überprüft und von der nach Ziff. 1.1.4 verantwortlichen Person unterschriftlich bestätigt wird“.

Die *IG eHealth* kritisiert bezüglich Ziffer 1.1.3.2.2, dass solche Einträge gemäss Artikel 9 Absatz 1 Buchstabe c EPDV gar nicht vorkommen dürften. Die Erläuterungen zur Verordnung würden andeuten, dass es technische Gründe geben könnte. Es gebe allerdings keine weiteren Details. Es wird die Streichung

dieser Ausnahme empfohlen. *HIN* bemängelt, dass der Begriff „rechtzeitig“ in Ziffer 1.1.3.2.3 Interpretationsspielraum offen lasse und schlägt, genau wie die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* folgende Formulierung vor: „[…] rechtzeitig, d.h. mindestens einen Monat vor dem Austritt, informiert werden und ausdrücklich darauf hingewiesen werden, dass die Dokumentenablage der austretenden Gesundheitseinrichtung auf den Austrittszeitpunkt gelöscht werden“. Ähnlich fordert der Kanton AR, dass der Begriff „rechtzeitig“ weiter ausdifferenziert wird. 6 Kantone[82] wünschen folgende Formulierung für Ziffer 1.1.3.2.3: „l'information en temps utile des patients par les professionnels de soins concernés“. Die *Tessaris* schreibt, dass nicht klar sei, welche Rechte und Ansprüche der / dem über den Austritt der Gesundheitseinrichtung informierten Patientin / Patienten zustehen. Es wird folgende Formulierung vorgeschlagen: „[…] Patienten in textlich nachweisbarer Form rechtzeitig informiert und über die ihnen nun verfügbaren Optionen aufgeklärt werden“.

1.1.4: Die *FMH* bemängelt, dass Ziffer 1.1.4 viele prozessuale Unklarheiten beinhalte, womit eine Präzisierung nötig sei. Die *K3*, der *VZK* und der *VAKA* fordern die Streichung von Ziffer 1.1.4.2.2. Die *BFH* weist darauf hin, dass gemäss Artikel 8 Buchstabe e EDPV die Zusammensetzung der Gruppen von Gesundheitsfachpersonen „jederzeit“ nachvollziehbar sein müsse. Hier stehe nun „vierteljährlich“. Eine Bewirtschaftung „jederzeit“ würde sehr anspruchsvoll sein, wenn es überhaupt machbar sei. „Vierteljährlich“ erscheine dabei etwas realistischer, der Widerspruch mit der Verordnung bleibe jedoch. Die *Tessaris* macht darauf aufmerksam, dass die mindestens zweimal pro Jahr durchzuführende Überprüfung und Bestätigung der Aktualität und inhaltlichen Korrektheit der im zentralen Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen registrierten Daten ein ausserordentlich aufwändiger Prozess sei. Es bleibe unklar, wie diese Überprüfung durchgeführt werde. 6 Kantone[83] weisen darauf hin, dass die Gemeinschaften nicht die Mittel hätten, um die Daten „zu überprüfen und zu bestätigen“, sondern und müssen sich auf die Angaben der Einrichtungen und Gruppen stützen. Sie schlagen folgende Formulierung von Ziffer 1.1.4 vor: „Chaque institution ou groupe enregistré dans le service de recherche central (.) doit: 1.1.4.1 désigner en son sein un répondant chargé de communiquer les changements intervenant dans les données à la communauté; 1.1.4.2 communiquer dans les trente jours à la communauté tous les changements intervenus dans les données enregistrées. 1.1.4.2.1 abrogé, 1.1.4.2.2 abrogé“.

1.2 Verwaltung von Gesundheitsfachpersonen (Bst. a bis d)

6 Kantone[84] wiederholen ihre Stellungnahme von Ziffer 1.1 in Bezug auf Ziffer 1.2.

1.2.2: Die *FMH* bezeichnet Ziffer 1.2.2.1 als nicht praktikabel und fordert deren Streichung. Im Zuge von Ziffer 1.2.2.3 gebe es Überschneidungen mit der EPDV. Die Überprüfung, ob es sich um eine Gesundheitsfachperson handle, habe durch qualifizierte Stellen zu erfolgen. Ausserdem müssen die Berufsgruppen unterschieden werden. Es wird eine klare Regelung auf Ebene EPDV gefordert. Des Weiteren schreibt die *FMH* bezüglich Ziffer 1.2.2.4, dass das IDM bei der Herausgabe registriert werden müsse, was ebenfalls einer klaren Regelung auf Ebene EPDV bedürfe. Zusätzlich stellt die *FMH* in ihrer Stellungnahme einige Fragen zu Ziffer 1.2.2.5 und fordert, dass es eine generelle Regelung der Prozesse auf Ebene EPDV gibt. Für 6 Kantone[85] ist Ziffer 1.2.2.4 unklar. Wenn ein IDM nicht registriert sei, dann könne es nicht verwendet werden. Das Vokabular (Identifikation oder Authentifizierung?) solle klargestellt und die Bedeutung in Bezug auf den Begriff „garantir“ von Ziffer 1.2.2 geklärt werden. Die Kantone *FR*, *GE*, *VS*, *VD* und *JU* schreiben zudem, dass das MedReg nicht unbedingt die aktuellsten Daten beinhaltet. Daher müssen diese Daten auch nicht systematisch übernommen werden. Der entsprechende Satz in Ziffer 1.2.2.5 sei dementsprechend zu streichen. Die *IG eHealth* und die *Post* fragen, ob die Register MedReg etc. nicht Bestandteil des Abfrageservices HPI seien und ob sie separat an den HPD angebunden werden müssten. Zudem sehen sie einen Widerspruch mit dem Gesetz. Die Gemeinschaften seien für die Daten zuständig. Die Register hätten eine andere Ownerschaft. Hier stelle sich

82 FR, NE, GE, VS, VD, JU
83 FR, NE, GE, VS, VD, JU
84 FR, NE, GE, VS, VD, JU
85 FR, NE, GE, VS, VD, JU

die Frage, wer das Recht bei widersprüchlichen Daten habe und bei Konflikten entscheide. Es gelte dies zu klären. Im Weiteren seien die Hilfspersonen ebenfalls in den Abfragedienst der Gesundheitseinrichtungen aufzunehmen, damit diese Gemeinschaften übergreifend identifizierbar und für die Patientin / den Patienten erkennbar werden. Die *Post* schreibt zudem, dass die Ausgabe und Verwaltung der Authentisierungsmittel für Mitarbeitende der Gesundheitseinrichtung an dieser Stelle nicht erwähnt werde und stellt die Frage, ob die Gemeinschaft das nicht weiter delegiere. Die *STSAG* wünscht die Sicherstellung, dass die Abfragedienste nach Ziffer 1.2.2.5 eine weitestgehend automatische Verarbeitung von Eintritten und Austritten von Gesundheitsfachpersonen erlauben. Die *Tessaris* wünscht folgenden Zusatz für Ziffer 1.2.2.5: „[…] von dort zu übernehmen und bei Änderung der Eintragungen in den betreffenden Registern nachzuführen". *SCH* kritisiert, dass Schnittstellen zu den Berufsregistern erstellt werden, da dies unnötig die Kosten erhöhe. Es wird deshalb die Streichung des zweiten Satzes von Ziffer 1.2.2.5 gewünscht.

1.2.3: 6 Kantone[86] fragen, wie der Zugang überprüft werden könne und ob es darum gehe, zu überprüfen, ob eine Gesundheitsfachperson, die auf das elektronische Patientendossier zugegriffen hatte, auch das Recht dazu hatte. Dieser Schritt werde bei Durchdringungstests geprüft aber nicht bei einem „Prozess für die Verwaltung von Gesundheitsfachpersonen". Ziffer 1.2.3.2 sei dementsprechend zu streichen. Zudem betrachten sie Ziffer 1.2.3.3 als unklar und wünschen deshalb Ausführungen dazu. *SBC* ist der Meinung, dass die Dokumentation über eine Patientin / einen Patienten nicht für die Ewigkeit in den Datensicherungsmedien (back-up Datei) gespeichert sein solle, wenn sie / er dies nicht möchte. Sonst bestehe stets das Risiko, dass bösartig Daten aus dem Backup genutzt werden, obwohl geglaubt werde, dass alles gelöscht sei. Die Daten seien für den Rechtsbeweis zudem immer noch in dem Primärsystem. Es wird folgender Text gefordert: „Datensicherungsmedien, die älter als 2 Jahre sind, sollten gelöscht werden. Es soll dabei sichergestellt werden, dass alle aktuellen Daten in Datensicherungsmedien, die weniger als 2 Jahre alt sind, auch gesichert sind". Die *Post* fragt im Rahmen von Ziffer 1.2.3, was mit Leistungserbringern in zwei Gemeinschaften passiere und wie es geführt werde. Unklar sei, ob der Datensatz dupliziert werde und wenn ja, wer für die Pflege verantwortlich ist. Für die *IG eHealth* und die *Post* ist die Anforderung gemäss Ziffer 1.2.3.3 nicht nachvollziehbar. Es müsse etwas gefordert werden, das auch umsetzbar sei. Die *Tessaris* verweist unter Ziffer 1.2.3.1, für die Daten in den in 1.2.2.5 erwähnten medizinischen Registern, auf die Empfehlung zu Ziffer 1.2.2.5. Bezüglich Ziffer 1.2.3.2 könne, wie in Ziffer 1.1.4.2 dargestellt, die Überprüfung, je nach den dafür eingesetzten und zugelassenen Mitteln und Verfahren, sehr aufwändig ausfallen. Für Ziffer 1.2.3.3 wird zudem folgender Zusatz gewünscht: „Die Zugriffsrechte gemäss den in Artikel 1-3 EPDV festgelegten Kategorien und Optionen angepasst werden". Die *FMH* fragt bezüglich Ziffer 1.2.3.3, woran die Zugriffsrechte angepasst werden.

1.2.4: Die Kantone *GE*, *VS*, *VD*, *JU* und *NE* weisen darauf hin, dass in der französischen Version bei Ziffer 1.2.4.2 zweimal aneinander „du patient" steht, womit es einmal zu löschen sei. Die *Tessaris* schreibt, dass nach hier vertretener Auffassung die Patientinnen / Patienten über den Ein- und Austritt von Gesundheitsfachpersonen informiert werden sollten und fordern folgende, zusätzliche Ziffer 1.2.4.4: „die Patientinnen und Patienten über den Eintritt sowie den Austritt einer Gesundheitsfachperson in die betreffende Gemeinschaft in textlich nachweisbarer Form informiert werden und ihre Optionen betreffend Zugriffsrechte ausüben können".

1.3 Verwaltung von Hilfspersonen von Gesundheitsfachpersonen

Die *IG eHealth* und die *Post* machen geltend, dass gemeinschaftsinterne Vorschriften nicht in den Geltungsbereich des EPDG fallen, weswegen dazu auch keine Vorschriften gemacht werden sollten. Der Scope der EPDV und der TOZ sei zu klären. Der *VAKA* schlägt im Sinne einer Vereinfachung vor, dass Hilfspersonen fakultativ umzusetzen seien und 1.3 somit gestrichen werden solle. Gemäss der *Insel* bedeute die Verwaltung von Hilfspersonen ein unverhältnismässig grosser Aufwand und die *IG eHealth* schreibt, dass Hilfspersonen auch übergreifend zu verwalten seien, um diese der Patientin / dem Patienten erkennbar zu machen. Die *IG eHealth* fordert die Streichung von Ziffer 1.3.1 und die *Insel* die

[86] FR, NE, GE, VS, VD, JU

Streichung von Ziffer 1.3. Für *HIN* ist es unklar, wie weit der Begriff "Hilfspersonen" gehe. Vermutlich seien MPA, PflegerInnen, u.ä.m gemeint. Vermutlich implizit nicht gemeint seien bspw. Köche eines Heims, Putzpersonal, Verwaltung etc. Es stelle sich die Frage, ob Leitlinien hilfreich wären. Die *STSAG* ist der Ansicht, dass Hilfspersonen nur verwaltet werden müssen, wenn sie auch in die Datenbehandlung eingebunden sind und schlägt folgenden Zusatz für Ziffer 1.3.1 vor: „[…] werden können, sofern diese (die Hilfspersonen) in die Bearbeitung der Daten im elektronischen Patientendossier direkt eingebunden sind". Gemäss der *FMH* müssen die Prozesse zur Verwaltung von Hilfspersonen in den Grundanforderungen einheitlich auf Verordnungsstufe geregelt werden und dürfen nicht von Gemeinschaft zu Gemeinschaft unterschiedlich sein. Ausserdem müsse klar definiert sein, welche Personen unter welcher Verantwortung Zugang zum elektronischen Patientendossier haben. Es wird bezüglich Ziffer 1.3.2.1 eine klare Regelung auf Ebene EPDV vorgeschlagen. Die *BFH* plädiert bezüglich den Ziffern 1.3.2 und 1.3.2.1 dafür, dass für Hilfspersonen ebenfalls Metadaten definiert werden. So seien insbesondere Administratoren und Supporter zu nennen, die Zugriff benötigen und auch haben werden. Der *VGIch* befürchtet, dass die aktuelle Verwaltung von Einzelpersonen, von Gruppen und Hilfspersonen in Spitälern, wie verlangt nur unter grössten Aufwänden bzw. gar nicht möglich sei, da dies nicht der gelebten und erprobten Praxis im Spital bzgl. Umgang mit elektronischen Hilfsmitteln entspreche. Der Spital solle als „Trusted Domain" betrachtet werden. Das *KSSG* schreibt, dass die Hilfspersonen gemäss Verordnung nicht mit den zentralen Diensten synchronisiert werden sollen. Dadurch könne die Patientin / der Patient die Hilfsperson vom Zugriff nicht ausschliessen. Dies führe die Selbstbestimmungsregelung ad absurdum. Zum Zweiten werde die Patientin / der Patient verwirrt, wenn in den Zugriffsprotokollen Zugriffe der Hilfsperson angezeigt werden, die ihr / ihm nicht beim Setzen der Berechtigung bekannt sind. Auch Hilfspersonen sollen im HPD geführt und mit den zentralen Diensten synchronisiert werden. Der Artikel sei zu löschen. Ziffer 1.2.3.3 sei ebenfalls nicht nachvollziehbar. Zugriffsrechte im elektronischen Patientendossier würden von Patientinnen / Patienten verwaltet. Sie fragen, welche Verwaltungsprozesse dabei zu einer Anpassung von Zugriffsrechten führen sollen und sprechen sich für die Löschung dieser Anforderung aus. Die *OFAC* gibt zu bedenken, dass die Hilfspersonen nicht in den Abfragediensten registriert seien, was dazu führe, dass sie nicht an dem Austausch zwischen den Gemeinschaften teilnehmen können. In verschiedenen Berufen des Gesundheitswesens werde die ganze Verwaltungsarbeit des Gesundheitsdossiers an die Hilfspersonen delegiert. Das heisst, dass ein gutes Management des Dossiers einen gewissen Austausch mit anderen Gesundheitsdienstleistern erfordern wird, die Hilfspersonen jedoch nicht ermächtigt sein werden. Diese Situation wäre eine Verschlechterung gegenüber dem heutigen System. Laut der *OFAC* könne die Eignung, einen intergesellschaftlichen Austausch vorzunehmen, nur von der Gesundheitsfachperson, die für die Hilfspersonen verantwortlich ist, bewertet und entschieden werden. Gemäss Artikel 2 Buchstabe b EPDG sollen die Hilfspersonen im zentralen Abfragedienst registriert sein und die von der Patientin / dem Patienten delegierte Rechte bekommen. Es könne in der Praxis folgendes passieren: Die Gesundheitsfachpersonen werden ihre IDM mit dem Passwort an die Hilfspersonen weitergeben, was Probleme verursachen könne.

1.4 Identifikation und Authentisierung (Art. 8 Bst. d)

1.4.1 / 1.4.2: *HIN* schreibt, dass in Ziffer 1.4.1 explizit nur Gesundheitsfachpersonen erwähnt seien, in Ziffer 1.4.2 auch Hilfspersonen. Es werde davon ausgegangen, dass auch Hilfspersonen eine eigene Identität brauchen. Es sei wichtig, dass auch Hilfspersonen nur IDM nach Artikel 30 EPDV verwenden dürfen. Ziffer 1.4.1 solle folgendermassen ergänzt werden: „Für den Zugriff von Gesundheitsfachpersonen und Hilfspersonen auf das elektronische Patientendossier [...]". Gemäss der *IG eHealth* und der *Post* bestehe das Problem, dass spitalinterne Logins nicht mehr zulässig sind. Die *IG eHealth* fügt an, dass der Abschnitt nur die Anforderungen der IDM für den Zugriff regle und fragt, welche Anforderungen für das Schreiben in ein Dossier gelten. Die *IG eHealth* fordert, dass nach kantonalem Recht genügende IDM der Organisationen für den Zugang zum elektronischen Patientendossier ebenfalls akzeptiert werden müssen. Ähnlich weist die *Post* darauf hin, dass die IDM der Organisationen akzeptiert werden müssen, da sie auch Vorschriften durch andere Gesetze haben. Die Zertifizierung der IDM innerhalb einer Organisation sei nicht Teil der EDPV. Zudem sei zu klären, ob eine Ein-Faktoren-Authentifizierung für Systeme in Ordnung sei, welche nur eine schreibgeschützte Ansicht der Gesundheitsakte ermögli-

che. Die *Tessaris* fordert folgende Anpassungen für Ziffer 1.4.2: „Gemeinschaften und Gesundheitseinrichtungen müssen sicherstellen, dass die eindeutigen Parameter der IDM von Gesundheitsfachpersonen und Hilfspersonen zuverlässig mit der registrierten Identität der jeweiligen Person in der Gemeinschaft bzw. der Gesundheitseinrichtung verbunden wird". Gemäss der *FMH* bestehen bezüglich Ziffer 1.4.2 Redundanzen. Sie schlagen eine klare Regelung auf Ebene EPDV vor.

1.4.3: Die *privatim* verweisen bezüglich Ziffer 1.4.3 auf ihre Ausführungen unter den allgemeinen Bemerkungen bei der EPDV. *HIN* begrüsst die verlangte, starke 2-Faktor-Authentisierung ausdrücklich. Gemäss der *STSAG* seien die Voraussetzungen an die Primärsysteme nicht akzeptabel in einer Verordnung über das elektronische Patientendossier, da die Institutionen hier schon kantonale Regeln befolgen müssen. Ziffer 1.4.3 sei wegen Eingriff in die Datenhoheit und –sicherheit der Primärsysteme ersatzlos zu streichen. Die *K3* und der *VZK* weisen darauf hin, dass die angeschlossenen Primärsysteme voraussichtlich zentrale und sehr häufig genutzte Systeme (KIS) seien, deren Zugang im normalen Gebrauch sehr rasch möglich sein müsse. Die Ziffer 1.4.3 sei so einzuschränken, dass sie nur für den Zugriff auf das elektronische Patientendossier aus einem Primärsystem gelte. Die *SGMI* und die *FMH* stellen fest, dass in Ziffer 1.4.3 / 1.4.3.1 Auflagen an die Primärsysteme gemacht werden. Sie fordern, dass keine Vorschriften für die Authentifizierung von Primärsystemen gemacht werden. Die *OFAC* macht geltend, dass die Gemeinschaften nichts bezüglich den Primärsystemen sicherstellen können, da sie weder deren Besitzer, noch dafür verantwortlich seien und sie sollen auch nicht die Verantwortung der Gemeinschaften werden.

Die *BFH* würde aufgrund Ziffer 1.4.3.1 folgern, dass die Zugriffsrechte von hochgeladenen Dokumenten, die also aus der eHealth-Plattform ins Primärsystem übernommen werden, folgen müssen. Es stelle sich die Frage, ob gemeint sei, dass ein „elektronisches Patientendossier-Fenster" im Primärsystem integriert ist, also gar nicht mehr im Primärsystem gearbeitet werde, sondern lediglich einen Browser-Inhalt zum elektronischen Patientendossier dargestellt werde. Der Unterschied wäre gross und hätte auf die Zugriffsrechte unmittelbare Konsequenzen, wie sie in der EPDV (Art. 8, Bst. e) bereits kommentiert wurden. In der Praxis seien entsprechende Authentisierungsverfahren in Primärsystemen jedenfalls kaum im Einsatz. Zudem arbeiten viele zusätzliche Personen – die nicht im HPI erfasst seien, weil sie keinen Zugriff auf das elektronische Patientendossier benötigen, mit dem Primärsystem und könnten dann Zugriff auf die hochgeladenen Dokumente haben. Das ginge dann am elektronischen Patientendossier vorbei. Das *KSSG* schreibt, dass Ziffer 1.4.3.1 die Auswirkung hätte, dass sich die Benutzer an jeder Applikation, die mit dem elektronischen Patientendossier in irgendeiner Art kommuniziert, sei dies als Dokumentenquelle oder als Dokumentenkonsument, mit einer 2-Faktor-Authenthifizierung anmelden müssten. Gemeinschaften müssen sicherstellen, dass alle technischen Systeme, wie z.B. Primärsysteme, beim Zugriff auf das elektronische Patientendossier (als Akteur IHE Document Consumer) ein starkes Authentifizierungsverfahren verwenden. Die *Post* und die *IG eHealth* weisen darauf hin, dass Ziffer 1.4.3.1 die Ziffer 1.4.1 aufweiche. Es sei Konsistenz in der TOZ herzustellen. Die *Post* fügt an, dass es nicht sein könne, dass einerseits die Verwendung von IDM zertifizierter Herausgeber gefordert werde und andererseits beliebige Verfahren akzeptiert werden nur, weil ein anderes Stück Software für den Zugriff genutzt wird. Ebenfalls bezüglich Ziffer 1.4.3.1 wünschen die *IG eHealth* und die *Post*, dass der Begriff „Bearbeitung" definiert wird. Gemäss dem *VGIch* stehe Ziffer 1.4.3.1 bezüglich angeschlossener Primärsystemen im Widerspruch zu Artikel 8 Buchstabe d EPDV und den entsprechenden Erläuterungen. Artikel 8 Buchstabe d und die Erläuterungen seien diesbezüglich anzupassen.

Der *VAKA* bezeichnet die in Ziffer 1.4.3.2 formulierte Forderung als nicht klar und es sei erstaunlich, dass in diesem Kontext die Primärsysteme explizit genannt seien. Je nach Forderung habe dies enorme Auswirkungen auf die Leistungserbringer. Die Forderung sei klarer zu formulieren. 6 Kantone[87] schreiben, dass die Gemeinschaften nicht sicherstellen („garantir") können, dass tausende verwendete Endpunkte vertrauenswürdig seien. Die Gemeinschaft könne nur die Gesundheitsfachpersonen informieren, weshalb Ziffer 1.4.3.2 zu streichen sei. Die *Post* und die *IG eHealth* fragen, ob die Forderung in Ziffer 1.4.3.2 bedeute, dass alle Gesundheitseinrichtungen, welche ein Primärsystem am elektronischen Pa-

[87] FR, NE, GE, VS, VD, JU

tientendossier anschliessen wollen, das entsprechende Primärsystem mit einem zertifizierten Herausgeber von IDM verknüpfen müssen. Das hätte Auswirkungen auf die Spitäler, die sich anschliessen müssen. Die Forderung sei klarer zu formulieren. Die *ahdis* bemängelt, dass nicht genau spezifiziert wird, wie der Endpunkt auszusehen habe. Dies sei zu präzisieren.

1.5 Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 8 EPDV Bst. a, c, e und f)

Die *FMH* schreibt bezüglich Ziffer 1.5, dass die vorgesehene Verwaltung von Gruppen nicht praktikabel und mit einer generellen Regelung auf Verordnungsebene zu ersetzen sei. Der Kanton *ZH* ist der Meinung, dass es weder erforderlich, noch zulässig sein dürfe, die Patientinnen / Patienten über jede Änderung der Zusammensetzung einer Gruppe zu informieren. Zudem sei der Begriff „verhältnismässig" unklar und unnötig. Ohnehin sei auf das Gebilde „Gruppen von Gesundheitsfachpersonen" zu verzichten. Es wird die Streichung von Ziffer 1.5 gefordert.

6 Kantone[88] machen geltend, dass die Gemeinschaften nicht für die Gruppen von Gesundheitsfachpersonen verantwortlich sein können. Sie können nur Kenntnis von deren Zusammensetzung nehmen. Bei Ziffer 1.5.1 sei der Textteil „sont responsable de la gestion" mit „sont responsable de l'administration" zu ersetzen. Sie schreiben auch, dass die Patientin / der Patient nicht auf die komplette Liste der Gesundheitsfachpersonen und der Hilfspersonen einer Gruppe oder einer Einrichtung zugreifen könne. Das sei heute nicht der Fall in der Praxis. Des Weiteren ändere die Zusammensetzung bei Einrichtungen oder grossen Gruppen täglich. Es sei nicht möglich, die Patientinnen / Patienten ständig über die Zusammensetzung der Gruppen zu informieren. Ein Spital sei ein Beispiel für eine Einrichtung, an welche die Patientinnen / Patienten Rechte erteilen können. Einrichtung in „verhältnismässige Gruppen" zu zerkleinern habe keinen praktischen Sinn. Die Patientin / der Patient müsste einer Vielzahl von Gruppen (z.B. Radiologie) Rechte erteilen, welche er nicht kenne. Folglich seien die Ziffern 1.5.2.1, 1.5.2.2 und 1.5.2.3 zu streichen. Die *OFAC* ist der Ansicht, dass die Anforderung gemäss Ziffer 1.5.2.2 nicht praktikabel sei, da Gruppen stark veränderbar seien. Bezüglich Ziffer 1.5.2.3 wird zudem kritisiert, dass eine verhältnismässige Grösse noch nichts Genaues bedeute. Die *BFH* bemängelt bezüglich Ziffer 1.5.2.1, dass der Begriff „jederzeit" nicht klar definiert sei. Hier komme insbesondere der Verwaltungsaufwand für grössere Gesundheitseinrichtungen zum Tragen. Falls mit „jederzeit" stündlich/täglich gemeint ist, wird es in grösseren Institutionen, mit in unterschiedlichen Bereichen arbeitenden Assistenzärzten, einen erheblichen Mehraufwand ohne erkennbaren Mehrwert geben. Ähnlich fragt der Kanton *AR*, was mit „jederzeit nachvollziehbar" gemeint sei und wünscht eine Präzisierung. Ebenfalls präzisiert werden solle der Teil „die Grösse von Gruppen verhältnismässig bleiben" aus Ziffer 1.5.2.3. Die *Post* schreibt, dass sie sich im Falle des Verzichts einer Definition von „verhältnismässig", an den Kundenwünschen ausrichten werde. Das *KSSG* bezeichnet den Begriff „verhältnismässig" ebenfalls als unpräzise und fordert die Streichung von Ziffer 1.5.2.3. Die Gruppen könnten in Fachbereiche unterteilt werden. Die *SGMI* schreibt, dass die Grösse der Gruppe abhängig von der Grösse der Institution sei und fordert eine Präzisierung oder die Streichung. Gemäss der *STSAG* sei der Aufwand bezüglich den Ziffern 1.5.2.1 und 1.5.2.2 unnötigerweise gross, die Zugriffe könne die Patientin / der Patient über das Protokollwesen einsehen und es sei nicht nachvollziehbar, weshalb die Patientin / der Patient alle potentiell einer Zugriffsgruppe zugeordneten Gesundheitsfachpersonen einsehen solle. Des Weiteren werde der Inhalt von Ziffer 1.5.2.3 bereits über die Benutzerberechtigungen in den Primärsystemen geregelt. Die Ziffern 1.5.2.1, 1.5.2.2 und 1.5.2.3 seien zu streichen. Der Kanton *TI* bezeichnet die Realisierung der vorgeschlagenen Verwaltung der Gruppen von Gesundheitsfachpersonen (1.5.2.1 und 1.5.2.2) als nicht einfach. In der alltäglichen Praxis hätten die Patientinnen / Patienten keinen Zugriff auf die Listen aller Fachpersonen von komplexen Einrichtungen (Spitäler), die Zugriff auf ihre Daten haben. An Orten mit hoher Personalfluktuation wäre diese Art von Echtzeitverwaltung zu aufwendig. Die beiden Ziffern seien zu streichen. Die *privatim* weisen darauf hin, dass für die Patientin / den Patienten nicht nur die jeweils aktuelle Zusammensetzung, sondern auch Veränderungen in der Gruppenzusammensetzung (Ein- und Austritte) nachvollziehbar sein sollten. Die Texte von den Ziffern 1.5.2.1 und 1.5.2.2 seien klarer auszuformulieren. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* wünschen, dass die Formulierung von Ziffer 1.5.2.2 in Bezug auf Artikel 8 Buchstabe f EPDV folgendermassen ergänzt wird: „[…] informiert

[88] FR, NE, GE, VS, VD, JU

werden können und informiert werden". Die *Insel* und der *VGIch* machen darauf aufmerksam, dass die Forderung gemäss Ziffer 1.5.2.2 in einem Spital nicht praktikabel resp. umsetzbar und somit zu streichen sei. Die *Tessaris* schlägt folgenden Zusatz für Ziffer 1.5.2.2 vor: „[…] in Gruppen von Gesundheitsfachpersonen und deren Austritt aus einer Gruppe von Gesundheitsfachpersonen informiert werden können". Ausserdem solle Ziffer 1.5.2.3 neu folgendes beinhalten: „[…] verhältnismässig bleiben und im Regelfall die Zahl von Angehörigen der Gruppe nicht überschreiten".

2. Datenhaltung und Datenübertragung (Art. 9 EPDV)

2.1 Löschen von Daten (Abs. 1 Bst. a und b)

6 Kantone[89] wiederholen bezüglich der Ziffer 2.1.1.1 ihre Stellungnahme von Artikel 20 EPDV. Sie schreiben zudem, dass die Daten nicht gelöscht werden müssen. Auf dem Papier oder in den Primärsystemen seien die Daten tatsächlich nicht gelöscht, weswegen es keinen Grund gebe, warum diese in einem Sekundärsystem gelöscht werden könnten. Ein grosser Vorteil des elektronischen Patientendossiers sei, dass den Patientinnen und Patienten eine Datenarchivierung über die Zeit angeboten werden könne. Im Gesundheitsbereich mache eine zeitliche Begrenzung von 10 Jahre keinen Sinn. Die Patientin / der Patient könne an einer medizinischen Behandlung vor 20 Jahren, oder sogar aus seiner Kindheit, interessiert sein. Der Kanton *NE* weist zudem darauf hin, dass der Artikel 64 des kantonalen Gesundheitsgesetzes zwar eine zeitliche Begrenzung von 10 Jahren für die Datenerhaltung vorschreibe, was aber eine minimale zeitliche Begrenzung sei, die noch nicht die „Informatisierung" der Dossiers betrachte. Die Frage, welchen Platz die Papierdossiers in der Gesundheitspraxis einnehmen, sei nicht in gleicher Art und mit den gleichen Bedingungen wie mit einem elektronischen Dossier zu behandeln. Es befinde sich in diesem (neuen) Kontext nahezu keine logistische sowie technische Beschränkung mehr, die der Gesundheitsfachperson einen Grund geben würde, die Elemente des Dossiers im Interesse der Patientin / des Patienten über 10 Jahre nicht zu behalten. Die *FMH* verweist an dieser Stelle auf ihre Bemerkungen zu den entsprechenden Verordnungsartikeln. Die *BFH* ist der Ansicht, dass die Vorstellungen über „meine Daten in meinem elektronischen Patientendossier" und die grundsätzliche Aufbewahrungspflicht im Gesundheitswesen aus Sicht eines Anwenders hier unverständlicherweise auseinander gingen. Auch wenn die Patientin / der Patient informiert wird und sie / er eine 10-jährige Verlängerung beantragen kann (Art. 9, Abs. 1, Bst.a), stellt sich die Frage, weswegen sie / er eine Entscheidung betreffend der Aufbewahrung ihrer / seiner Daten treffen müsse. Die Patientin / der Patient habe zudem ohnehin jederzeit die Möglichkeit, Dokumente zu löschen. Wenn es eine Vernichtungspflicht geben sollte, dann einen automatischen Übertrag in das Repository für die „privaten" Dokumente. Sollte es keine Vernichtungspflicht geben, sei die Vorgabe aus Ziffer 2.1.1.1 ersatzlos zu streichen. Die *medshare* betont an dieser Stelle, dass nur die Patientin / der Patient alleine entscheide, wann Dokumente aus den Dokumentenablagen und Registern gelöscht werden. Die *STSAG* schreibt, dass die Frist von 10 Jahren gemäss Ziffer 2.1.1.1 sinnvollerweise nur nach Beendigung der medizinischen Behandlung, welche bei chronischen Patientinnen / Patienten laufend erweitert werde, gelte. Alternativ könnten in der Registry nur Daten, die nicht älter als 10 Jahre sind, dargestellt werden. Die *Tessaris* schlägt vor, dass die Löschung von Patientendaten nach 10 Jahren als "Default Regelung" formuliert werden sollte. Gerade für Daten über den Verlauf chronischer Erkrankungen sei eine wesentlich längere Aufbewahrungsdauer üblich. Es wird folgender Zusatz für Ziffer 2.1.1.1 gewünscht: „[…] erfassten Daten unter Vorbehalt einer festgelegten längeren Aufbewahrungsdauer nach 10 Jahren vernichtet werden". Die *OFAC* fragt, was mit Daten sei, die auch nach den 10 Jahren noch relevant seien und verweisen auf das HMG, dessen letzte Revision vorschreibe, dass das Primärsystem eine Archivierung der Daten mit Bezug auf die Verwendung von Blutprodukten während 30 Jahren verlange.

6 Kantone[90] weisen bezüglich Ziffer 2.1.1.2 darauf hin, dass im Falle des Wunsches der Patientin / des Patienten zur Reaktivierung, oder aus forensischen Gründen, das elektronische Patientendossier nicht sofort gelöscht werden sollte, sondern eine Weile ausgeblendet sein müsse. Für *HIN* ist unklar, ob die Login-Daten in so einem Fall ebenfalls zu löschen seien. Der Text sage: "sämtliche Daten". Gemäss

89 FR, NE, GE, VS, VD, JU
90 FR, NE, GE, VS, VD, JU

Artikel 20 Absatz 1 sollen aber sämtliche Daten vernichtet werden, sofern sie nicht für die Erfüllung von Nachvollziehbarkeits- und Berichtspflichten benötigt werden. Es sei für Ziffer 2.1.1.2 dieselbe Formulierung wie in Artikel 20 zu verwenden. Die *Post* weist darauf hin, dass der Patientenindex eine Infrastruktur sei, die mehrfach genutzt werden könne. Sie fragt, ob es gestattet sei, nur die Identitäten aus dem MPI zu löschen, die im elektronischen Patientendossier genutzt wurden. Andere Identitäten die für andere Prozesse (z.B. Zuweisung, Überweisung) genutzt werden, blieben bestehen. Die gemeinsame Nutzung von Infrastruktur sei gemäss EPDG gestattet. Forderungen, die dies verhindern seien durch solche zu ersetzen, welche dies im angemessenen Rahmen erlauben. Der MPI solle eine Ausnahme bilden und Daten sollen gelöscht werden, wenn kein anderer Zweck bestehe. Gemäss dem *KSSG* haben die Vorgaben betreffend der Datenhaltung, wie z.B. in Artikel 9 Absatz 1 Buchstabe c EPDV und Ziffer 2.1.1.2.1 zur Folge, dass Anwendungsfälle, welche bereits eine Registry einsetzen, nicht mehr auf der bestehenden Infrastruktur betrieben werden können. Die Ausführungsbestimmungen hätten zur Folge, dass für das elektronische Patientendossier und alle restlichen Anwendungsfälle eine getrennte Infrastruktur aufgebaut werden müsse, was die Kosten verdopple. Ziffer 2.1.1.2.1 sei so umzuformulieren, dass eine logische Löschung für den Anwendungsfall „elektronisches Patientendossier" erfolgen muss, jedoch nicht eine physische Löschung. Damit solle sichergestellt werden, dass andere Anwendungsfälle weiterhin über die gleiche Infrastruktur abgebildet werden können. Des Weiteren würden die Vorgaben von Artikel 9 Absatz 1 Buchstabe c EPDV und Ziffer 2.1.1.2.2 zur Folge haben, dass die in den Spitälern bestehenden Archiv System nicht als IHE Repository für das elektronische Patientendossier verwendet werden können. Durch die Vorgaben müssen für die durch die Patientin / den Patienten eingestellten Dokumente, wie auch für die durch die Gesundheitsfachpersonen eingestellten Daten, ein separates Repository aufgebaut werden. Damit werde eine teure Infrastruktur insgesamt dreimal aufgebaut und enthalte zum Teil redundante Daten. Sollte mit dem Artikel 2.1.1.2.2 eine physische Löschung der Daten angestrebt werden, können die günstigeren Archivspeicher (z.B. Centera) nicht dafür verwendet werden. Die Auswirkungen auf die Kosten würden sich speziell dann zeigen, wenn auch radiologische Bilddaten im elektronischen Patientendossier abgelegt werden sollen. Computertomographie oder MRI-Untersuchungen seien oft mehrere Gigabyte gross und müssten redundant gespeichert werden. Der Artikel habe dementsprechend enormen Einfluss auf die Betriebskosten. Es wird beantragt, dass alle Daten im gleichen physischen Repository gespeichert werden können. Die Trennung und Löschung von Daten erfolge jeweils auf logischer Ebene für das elektronische Patientendossier. Die Anforderungen hinsichtlich Datenschutz und Datensicherheit wären auch mit einer logischen Trennung gegeben. Bezüglich Ziffer 2.1.1.2.3 weist das *KSSG* darauf hin, dass im Kanton St. Gallen seit mehreren Jahren ein MPI für die spitalübergreifende Kommunikation eingesetzt werde und beschreibt ebenfalls die Vorteile des MPI. Die aktuellen Ausführungsbestimmungen würden einen weiteren Betrieb des heutigen MPI verhindern, da die Patientin / der Patient im MPI nur geführt werden dürfe, wenn sie / er die Einwilligung zum elektronischen Patientendossier gegeben habe und sie / er müsse wieder gelöscht werden, wenn sie / er das elektronische Patientendossier löscht. Ein zweiter MPI nur für das elektronische Patientendossier aufzubauen sei nicht möglich, da es nur einen geben dürfe. Die Umsetzung der aktuellen Ausführungsbestimmungen wäre ein Rückschritt in den Behandlungsprozessen. Es wird beantragt, dass der MPI für das elektronische Patientendossier und auch andere Prozesse genutzt werden kann, jedoch für Patientinnen / Patienten ohne Einwilligung nicht mit der ID des elektronischen Patientendossiers der ZAS verknüpft werde. Bei Auflösung des elektronischen Patientendossiers werde einfach die Verknüpfung zur ID gelöscht.

Die *ISSS* weist darauf hin, dass in den Ziffern 2.1.1.1 und 2.1.1.2 von „Daten müssen vernichtet werden" die Rede sei. Es sei unklar, was dies konkret bedeutet und ob z.B. das (elektronische) Löschen ausreiche. Es wird vorgeschlagen, zur Regelung der Vorgaben bezüglich der Vernichtung eine Ziffer 2.1.1.3 aufzunehmen. Gemäss der *Tessaris* sollte sich die Pflicht zur Vernichtung insbesondere auch auf Sicherungsdateien und Back-up Kopien beziehen, da „sämtliche Daten" zu vernichten seien.

2.2 Dokumentenablage (Abs. 1 Bst. c)

Der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* weisen darauf hin, dass sich die Vorgaben gemäss Ziffer 2.2 bereits aus dem EPDG und der EPDV ergeben würden, weswegen sie zu streichen seien. Der

Kanton *AR* erachtet die Vorgabe gemäss Ziffer 2.2.1.1 als sinnvoll. Die *BINT*, die *Integic* und das *KSSG* schreiben wiederum, dass die Storage Architektur im Wandel sei und nicht in einer Verordnung festgeschrieben werden solle. 17 Stellungnehmende[91] befürchten, dass die Vorgabe zu einem hohen Aufwand bei den Leistungserbringern führe. Weiter kritisieren die *SGMI* und *FMH*, dass die Leistungserbringer aufgrund Ziffer 2.2.1.1 eine weitere, redundante Datenablage erstellen müssten, womit auch der bidirektionale Datenaustausch mit dem EPDG verkompliziert werde. Die *BFH* fragt, ob die Dokumentenablage in einer virtualisierten Umgebung betrieben werden dürfe. Die *SUVA* erachtet es als wenig sinnvoll, der Gemeinschaft die Architektur der Datenablage vorzuschreiben. Diese sei einem raschen Wandel unterworfen, weshalb es wenig Sinn mache, auf Verordnungsstufe Vorschriften aufzunehmen. Insgesamt sprechen sich 9 Stellungnehmende[92] für die Streichung von Ziffer 2.2.1.1 aus. Die *GKD* und 10 Kantone[93] fordern zumindest eine einfachere Regelung. Die Verwendung der auch für das KIS (der *ZAD* verwendet in seiner Stellungnahme das Wort „Primärsystem“) eingesetzten Dokumentenablage, allenfalls mit gewissen sicherheitstechnischen Vorgaben, sollte zulässig sein. Der Kanton *ZH* betont, dass die allfälligen sicherheitstechnischen Vorgaben nicht so restriktiv sein dürfen, dass ein Kostenschub bei den Leistungserbringern ausgelöst werde. *HIN* schreibt, dass hier eine logische Trennung genügen sollte und schlägt folgende Formulierung von Ziffer 2.2.1.1 vor: „Dokumente des elektronischen Patientendossiers jederzeit von anderen in der Datenablage gespeicherten Dokumenten getrennt werden können im Sinne einer kontrollierten logischen Trennung“. Für die *IG eHealth* und die *POST* ist unklar, was mit dem Wort „ausschliesslich“ gemeint sei, 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. Sie schlagen die Streichung des Wortes „ausschliesslich“ aus Ziffer 2.2.1.1 vor.

Die *IG eHealth* ist der Meinung, dass bezüglich Ziffer 2.2.1.2 wohl Anhang 4 und nicht Anhang 3 gemeint sei, was korrigiert werden müsse. Die *Post* fragt, ob es gestattet sei, On Demand Dokumente ins elektronische Patientendossier einzubringen. Das Standard CDA-CH-MTPS basiere auf On Demand Dokumente. Zudem gibt sie zu bedenken, dass die Vorschriften extrem restriktiv seien und jegliche Adaption von neuen Technologien verhindern würde, was zu vermeiden sei. Falls mit den „zugelassenen Dateiformaten“ die Liste gemäss Ziffer 1.9 (MIME-Typ des Dokuments) des Anhangs 3 gemeint sei, macht der Kanton *ZH* geltend, dass es problematisch sei, die Zahl der zugelassenen Dateiformaten einzuschränken. Eine Konvertierung in ein zugelassenes Format sei erstens technisch nicht immer machbar und dürfte zweitens auch nicht erforderlich sein. Insbesondere Formate wie PNG oder SVG, aber auch Textdokumente sollten unterstützt werden. Im Übrigen sei die Angabe von Formaten wie TIFF oder XML zu wenig präzise. Ziffer 2.2.1.2 sei zu überarbeiten oder zu streichen.

Die Kantone *GE*, *VD*, *VS*, *JU* und *FR* bezeichnen Ziffer 2.2.1.3 als zu restriktiv. Heute existiere die Ausprägung PDF/A-3, eingeführt durch die Revision der ISO 19005. Ausserdem könnte auch die Ausprägung PDF/X (ISO 15930) verwendet werden. Diese Normen werden ständig weiterentwickelt. Technische Details hätten keinen Platz in einer verbindlichen Gesetzgebung, weswegen die Ziffer zu streichen sei. Die *IG eHealth* schreibt, dass die Einschränkung auf die Ausprägung PDF/A-1 oder PDF/A-2 zu einer zwingenden Transformation der Daten führen könne. Diese Transformation berge das Risiko eines Informations- 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 werde. Ziffer 2.2.1.3 sei dementsprechend zu streichen. Gemäss der *Integic* seien die Angaben zu PDF/A-1 oder PDF/A-2 zu unpräzise, das sich innerhalb dieser beiden die Sub-Versionen hinsichtlich Anforderungen und vor allem Lesbarkeit stark unterscheiden. PDF/A-1a sei bspw. für Langzeitarchivierung und barrierefreie Anwendungen, während PDF/A-1b dies nicht ermögliche. PDF/A-1 bzw. PDF/A-2 seien eher als teilweise überschneidende, evolutionäre Technologien zu

[91] K3, VZK, SGMI, FMH, ZAD, GDK, BL, GL, LU, OW, UR, ZG, FR, NW, ZH, TG, SZ
[92] BINT, Integic, VAKA, SGMI, FMH, KSSG, K3, VZK, SUVA
[93] GDK, ZAD, BL, GL, LU, OW, UR, FR, NW, ZG, ZH, SZ

verstehen, während die Unterversionen die Semantik konkreter regeln[94]. Die *Integic* fordert die Präzisierung der erlaubten Unterversionen von PDF/A-1 und PDF/A-2. Der Kanton *ZH* weist darauf hin, dass die PDF-Formate PDF/A-1 und PDF/A-2 für die Archivierung entwickelt worden seien. Falls vorgeschrieben werde, dass nur diese Formate verwendet werden dürfen, führe dies dazu, dass viele Dokumente konvertiert werden müssen, ohne dass dafür ein Bedarf bestehe. Es sei für die Zwecke des elektronischen Patientendossiers nicht erforderlich, diese Formate vorzuschreiben, weshalb die Vorgabe zu streichen sei. Die *FMH* fragt bezüglich Ziffer 2.2.1.3, ob man nicht die Version PDF/A-3 habe. Es seien in der Gesetzgebung keine so genauen Spezifikationen zu machen, vor allem in einem Gebiet, welches sich ständig fortentwickelt. Die *Post* schreibt, dass es sich bei Ziffer 2.2.1.3 um eine unnötig einengende Anforderung handle. Die Daten sollen nach 10 Jahren gelöscht werden. Die meisten Anwendungen würden nicht standardmässig das Archivierungsformat erstellen. Sie beantragt, dass das erwartete Systemverhalten definiert wird. Das System solle keine Transformation des Formats vornehmen, weil dabei immer das Risiko bestehe, dass die Daten verloren gehen oder geändert würden, welche für die Behandlung relevant sein könnten.

2.3 Verwaltung auf Wunsch der Patienten (Abs. 2)

Die *FMH* verweist bezüglich der Ziffer 2.3 auf ihre Bemerkungen zu den entsprechenden Verordnungsartikeln. Die *OFAC* schreibt, dass man zusätzlich zu der Matrix mit der Vertraulichkeitsstufe / Auskunftsrechte, um eine flexible („à la carte"-) Verwaltung der Dokumententypen pro Patientin / Patient bitte. Zusätzlich zu der surrealen technischen Sichtweise, sei es aus medizinischer Sichtweise wahrscheinlich gefährlich, wenn ein unvollständiges elektronisches Patientendossier gepflegt werde. Dies aufgrund der Wahrscheinlichkeit, dass die Gesundheitsfachpersonen in gewissen Notfallsituationen medizinische Entscheidungen nur auf Basis des elektronischen Patientendossiers treffen werden. Eine solche Komplexität wäre nicht nur nutzlos und unrealisierbar, sondern wahrscheinlich auch gefährlich für die Gesundheit der Patientin / des Patienten. Die *IG eHealth* und die *Post* kritisieren, dass die Forderung gemäss 2.3.1.1.1 zu wenig klar formuliert sei. Die Publikation von Dokumenten sei Sache der Gesundheitsfachpersonen und nicht der Gemeinschaften. Grundsätzlich sollte die Patientin / der Patient die Gesundheitsfachpersonen instruieren und nicht die Gemeinschaften. Der Begriff "bestimmte" könne von den Gemeinschaften zudem nicht interpretiert werden. Die Anforderung müsse klarer formuliert werden, denn so könne sie nicht umgesetzt werden. Das *KSSG* bemängelt, dass Ziffer 2.3.1.1.1 nicht umsetzbar sei. Wenn bspw. eine Patientin / ein Patient den HIV Test, welcher Bestandteil einer kompletten Laboranalyse (Analyse-Reihe) ist, nicht im elektronischen Patientendossier veröffentlicht haben möchte, könne entweder der komplette Laborbefund oder gar kein Laborbefund im elektronischen Patientendossier veröffentlicht werden. Die Ziffer verlange zudem, dass ein Arzt vor der Veröffentlichung eines Dokumentes jedes Mal das Einverständnis der Patientinnen / Patienten einholen müsste. Es wird beantragt, dass Artikel 9 Absatz 2 Buchstabe a EPDV und Ziffer 2.3.1.1.1 zu streichen seien, da die Patientin / der Patient jederzeit die Möglichkeit habe, seine Vertraulichkeitsstufe auf geheime Daten zu setzen. Zudem müssten die Begriffe „Daten" und „Dokumente" genauer definiert werden. Die *STSAG* sieht in Ziffer 2.3.1.1.1 einen unverhältnismässigen Aufwand für die Gemeinschaften. Diese Aufgabe könne die mündige Patientin / der mündige Patient im Bedarfsfall selbst übernehmen. Da die Anlaufstelle der Patientin / des Patienten zudem die Stammgemeinschaft sei, müsse diese Aufgabe wenn schon, dann der Stammgemeinschaft übertragen werden. Es wird die ersatzlose Streichung der Ziffer gefordert. 6 Kantone[95] sind der Ansicht, dass die Patientin / der Patient, wenn sie / er die Aufnahme ihrer / seiner Daten im elektronischen Patientendossier nicht wünscht, dies bei der entsprechenden Gesundheitsfachperson anbringen müsse. Die Gemeinschaft könne die Registrierung von medizinischen Daten nicht verhindern. Sie fordern die Streichung von Ziffer 2.3.1.1.1.

Dieselben 6 Kantone beantragen auch die Streichung von Ziffer 2.3.1.1.2, da die medizinischen Daten nicht vernichtet werden müssen und somit eine Bitte um Verlängerung keinen Sinn mache. Dementsprechend schreiben sie, dass eine Patientin / ein Patient in ihrem / seinem elektronischen Patienten-

[94] http://www.pdfa.org/wp-content/uploads/2011/10/Flyer-PDFA2-Uebersicht-DE.pdf
[95] FR, NE, GE, VS, VD, JU

dossier keine medizinischen Daten löschen können sollte. Die Löschung der Daten aus einem Sekundärsystem mache ausserdem keinen Sinn, da diese im Primärsystem verbleiben. Eine Patientin / ein Patient, die / der seine Daten verstecken möchte, könne diese als geheim klassifizieren. Im Falle eines gerichtsmedizinischen Problems werde es wichtig, dass bekannt sei, an welchem Datum eine Patientin / ein Patient seine Daten ausgeblendet hatte und ob eine Gesundheitsfachperson vorgängig die Möglichkeit hatte, diese zur Kenntnis zu nehmen. Die Ziffer 2.3.1.1.3 sei also ebenfalls zu löschen. Die *K3* und der *VZK* bemängeln bezüglich den Ziffern 2.3.1.1.1 – 2.3.1.1.3, dass verbindliche Regelungen für Dokumente, welche aus einer anderen Gemeinschaft (über XCA) in dem elektronischen Patientendossier zu finden sind, fehlen würden. XCA sei ein „reiner Lesezugriff" ohne Schreib-, Mutations- oder Löschrechte. Die vollständige Löschung benötige entsprechende Regelungen, welche für den schweizweiten Verbund der Gemeinschaften, dem Vertrauensraum des elektronischen Patientendossiers, gelten. Diese Anmerkung gelte entsprechend auch für weitere Ziffern. Sie schlagen die Schaffung entsprechender Regelungen vor. Gemäss dem Kanton *ZH* sei es bezüglich Ziffer 2.3.1.1.3 nicht erforderlich, dass die Patientin / der Patient die Vernichtung von Daten aus dem elektronischen Patientendossier verlangen könne. Das elektronische Patientendossier solle vollständig bleiben. Nur so sei sichergestellt, dass die Daten, bspw. für eine Rechtsstreitigkeit, zur Verfügung stehen. Es sei ausreichend, dass die Patientin / der Patient diese Daten der Vertraulichkeitsstufe „geheime Daten" zuordnen kann. Die Ziffer sei dementsprechend zu streichen. Die *medshare* betont betreffend Ziffer 2.3.1.1.2, dass ein elektronisches Patientendossier von der Eröffnung bis zum Tod der Patientin / dem Patienten gehöre und aus diesem Grund nur sie / er das Recht habe, es zu löschen. Die Ziffer sei zu streichen. Die *privatim* weisen bezüglich Ziffer 2.3.2 auf ihren Kommentar in den allgemeinen Bemerkungen zur EPDV hin.

2.4 Umsetzung der Vertraulichkeitsstufen (Abs. 3 Bst. a)

Die *K3*, der *VZK*, der *ZAD* und der Kanton *ZH* schreiben, dass sich die Vorgaben bereits aus dem EPDG und der EPDV ergeben würden. Der *VAKA* schlägt vor, dass die Patientin / der Patient die Möglichkeit haben solle, keine Berechtigungen zu vergeben. Die *OFAC* schreibt, dass die Übersetzung der Vertraulichkeitsstufen ins Französische eine Katastrophe sei. Einige Stufen tragen den Namen einer Kategorie von persönlichen Daten, welche in Artikel 3 DSG definiert sei. Nach dem gesunden Menschenverstand gehören die meisten Daten tatsächlich mehreren Kategorien an. Medizinische Daten seien nützlich und zudem auch sensibel. Es sei nicht logisch, dass sich die medizinischen Daten in einem elektronischen Patientendossier erst auf der zweiten Stufe befinden und von 2 Klassen übertroffen werden. 6 Kantone[96] fordern, dass sämtliche Stufen und deren Verwendung in der Praxis weiter erläutert und durch konkrete Beispiele vervollständigt werden müssen. Gemäss der *Integic* impliziere Ziffer 2.4.1.3, dass die Gesundheitsfachpersonen die als „sensibel" eingestuften Daten in Folge, abhängig von den gewählten Zugriffseinstellungen, nicht mehr einsehen könnten. Es müsse klargestellt werden, dass für Gesundheitsfachpersonen die Änderung der Vertraulichkeitsstufen die entsprechende Berechtigung erforderlich sei bzw. die Änderung eine eigene Berechtigung darstelle. Die *SQS* weist darauf hin, dass die Beschreibungen der erwähnten 4 Vertraulichkeitsstufen im Anhang 3 Metadaten, 1.5 Vertraulichkeitsstufe übersetzt seien. Die Vertraulichkeitsstufe mit dem Code 30002 sei Englisch mit «useful medical data» und Deutsch mit «nützliche Daten» beschrieben. Die anderen Codes hätten in Englisch und Deutsch die gleiche Beschreibung, was auch in diesem Fall vorzunehmen sei. Die *STSAG* fordert bezüglich Ziffer 2.4.1 folgende Formulierung: „Stammgemeinschaften müssen […]" und bezüglich Ziffer 2.4.1.3 schreibt sie, dass diese Funktion automatisiert werden und über entsprechende Dienste realisierbar sein müsse.

2.5 Durchsetzen der Zugriffsentscheidung (Abs. 3 Bst. a)

Die *FMH* weist darauf hin, dass es sich nicht um eine „Zugriffsentscheidung der Stammgemeinschaft" handle, sondern um eine Prüfungsanfrage, die positiv beantwortet werden müsse. An anderer Stelle würde der Begriff „Authorisierungsentscheid" verwendet. Die Begrifflichkeit sei zu überarbeiten und einheitlich zu verwenden. Die Kantone *GE*, *FR*, *VS*, *VD* und *JU* bezeichnen Ziffer 2.5.1.1 als unklar. Sie fragen, ob die Gemeinschaften die Stammgemeinschaft anfragen müssen, welche Rechte die Patientin / der Patient gewähre und in welcher Form. Diese Rechte sind in einem Berechtigungsregister enthalten,

[96] FR, NE, GE, VS, VD, JU

verbunden mit dem MPI, auf welches die Gemeinschaften Zugriff haben müssen. Der Use Case sei zu klären und präzisieren.

2.6 Notfallzugriff (Abs. 3 Bst. a)

Die *FMH* verweist betreffend der Ziffer 2.6 auf die Bemerkungen zu entsprechenden Verordnungsartikeln und der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* betrachten die unter der Ziffer aufgeführten Vorgaben als zu kompliziert und fordern dementsprechend eine Vereinfachung. Die *STSAG* ist der Meinung, dass die Aufgaben gemäss Ziffer 2.6.1 an die Stammgemeinschaften übertragen werden sollten. Der Kanton *TI* schreibt, dass die Vorgaben in einer Notfallsituation nicht praktikabel seien. Das Verfahren müsse mittels einer vorgegebenen Antwort vereinfacht werden. Die Gesundheitsfachperson, die den Zugriff im Notfall erzwingt, müsse dies im Nachhinein begründen. Ähnlich fordern die *SGMI*, die *BINT*, die *IG eHealth*, die *SUVA* sowie die *FMH*, dass bezüglich Ziffer 2.6.1.1 das Wort „vorgängig" mit „nachträglich" zu ersetzen sei resp. eine nachträgliche Begründung ausreiche. Die *medshare* macht bezüglich Ziffer 2.6.1.1 darauf aufmerksam, dass im Notfall jede Minute für die Patientin / den Patienten zähle. Aus diesem Grund seien die medizinischen Leistungen klar prioritär vor der Administration. Der Erlasstext sei folgendermassen anzupassen: „innert 24 Stunden eine Begründung […]". Der *VAKA* wiederum fordert, dass gänzlich auf eine Begründung zu verzichten sei, weshalb Ziffer 2.6.1.1 gestrichen werden könne.

Das *USB* spricht sich dafür aus, den Zugriff für Gesundheitsfachpersonen in Notfallsituationen so einfach wie möglich zu halten. Zu diesem Zweck wird die Zusammenlegungen der Ziffern 2.6.1.1 und 2.6.1.2 vorgeschlagen mit folgender, neuen Formulierung: „der Notfallzugriff in der Protokollierung als solcher dokumentiert ist und sich von den übrigen Zugriffen unterscheiden lässt". Die *IG eHealth* und die *Post* weisen darauf hin, dass die Forderung gemäss Ziffer 2.6.1.2 die Arbeit mit dem elektronischen Patientendossier in einer Notfallsituation sehr aufwändig mache. Die Benutzerfreundlichkeit sei zu beachten. Sie beantragen, dass es für die Gesundheitsfachpersonen jederzeit klar sichtbar sein müsse, dass ein Notfall deklariert ist und dass die Zugriffe mit Notfallautorisierung ausgeführt werden. Dies sei analog zu den von Patientinnen / Patienten beigebrachten Dokumenten. Dort müsse die Gesundheitsfachperson auch nicht jedes Mal bestätigen, dass die Quelle der Daten bekannt ist. Gemäss der *SCH* müsse ein Notfallzugriff schnell gehen, die betroffene Gesundheitsfachperson sei bereits registriert. Die erschwerte Registrierung bringe keinen Zusatznutzen, da die Person bereits identifiziert sei. Ziffer 2.6.1.2. sei deshalb zu streichen. Die *SUVA* plädiert dafür, dass der Notfallzugriff unbürokratisch und schnell erfolgen müsse sowie eine Begründung auch nachgeliefert werden könne. Ziffer 2.6.1.2 solle folgendermassen lauten: „ein Notfallzugriff auch ohne nochmalige Bestätigung […]". Die *ISSS* fragt u.a., wie diese Notfallzugriffe vor Missbrauch geschützt werden sollen und wie es hier die genannte manuelle Interaktion genau aussehe. Der Prozess bedürfe einer detaillierteren Formulierung.

Die *SGMI* spricht sich dafür aus, das Wort „unverzüglich" in Ziffer 2.6.1.3 mit „nachträglich" zu ersetzen. Die *Post* fragt diesbezüglich, was „unverzüglich" bedeute und ob auch der postalische Weg gewählt werden könne. Die *FMH* schreibt, dass die systematische, nachträgliche Information und allfällige Begründung bei Verdacht auf missbräuchlichen Zugriff eine sachgerechte Lösung sei und genügen müsse.

Die *Integic* wünscht, dass Rahmenbedingungen, wie die Kontaktaufnahme zu erfolgen habe, ergänzt werden. *HIN* weist bezüglich Ziffer 2.6.1.4 darauf hin, dass die Information schützenswerte Daten enthalten könne, aber sie dürfe dann natürlich nur in Konformität mit den Anforderungen des Datenschutzes über entsprechend geschützte Kanäle erfolgen. Es solle folgende Änderung vorgenommen resp. Zusatz hinzugefügt werden: „[…](z.B. SMS, E-Mail, etc.) und schützenswerte Daten enthält, muss datenschutzkonform via geschützte Kanäle erfolgen. Andernfalls darf nur die Angabe, dass ein Notfallzugriff erfolgte, mit Datum und genauer Uhrzeit enthalten sein sowie der Hinweis, dass die genauen Umstände des Zugriffs dem elektronischen Patientendossier entnommen werden können". Ähnlich fordern die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* folgenden Wortlaut: „[…] übermittelt wird nur die Angabe, dass ein Notfallzugriff erfolgte, mit Datum und genauer Uhrzeit enthält sowie den Hinweis, dass die genauen Umstände des Zugriffs dem elektronischen Patientendossier entnommen werden können".

2.7 Überprüfung der Berechtigungssteuerung (Abs. 3 Bst. a)

Die *BINT* bemängelt, dass Ziffer 2.7 den Aufwand ins unendliche treiben könne, da das Szenario und die Funktionalität unbekannt seien. 6 Kantone[97] schreiben, dass der Rahmen der Testszenarien dem Ermessen der Zertifizierungsstelle und der Anbieter überlassen werden sollte. In Abhängigkeit der Anzahl der Tests sei eine Automatisierung nicht notwendig und verkompliziere die Struktur unnötig. Zudem habe die Art von Detail keinen Platz im verbindlichen rechtlichen Rahmen. Es wird die Streichung des Begriffes „automatisierter" aus Ziffer 2.7.1 gefordert. Die *privatim* fragen, auf welche Daten im Rahmen automatisierter Testszenarien zugegriffen werden können und durch wen. Sie wünschen die Spezifizierung der Regelung und weisen darauf hin, dass unautorisierte Datenzugriffe zu vermeiden seien. Die *SQS* fragt ihrerseits, wer bestimme, wann die Funktionalitäten und Regelauswertungen als korrekt betrachtet werden können. Die Regelung sei mit Ziffer 2.7.1.2 zu ergänzen und die zulässigen Werte für die Überprüfung festzusetzen bzw. zu bestimmen. Zudem ist zu definieren, wer für die Festsetzung dieser Werte zuständig ist.

2.8 Metadaten (Abs. 3 Bst. b)

Die *FMH* verweist bezüglich der Ziffer 2.8 auf ihre Bemerkungen zu den entsprechenden Verordnungsartikeln. *HIN* und die *SQS* vermuten, dass mit „Metadaten" Anhang 3 gemeint sei und nicht Anhang 4, was zu korrigieren sei. Ähnlich schreiben die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG*, dass hinsichtlich der Metadaten auf Anhang 4 der EPDV-EDI verwiesen werde. Im Anhang 4 würden jedoch die Austauschformate und nicht die Metadaten festgelegt. Es sei daher davon auszugehen, dass hier Anhang 3 gemeint sei. Die *IG eHealth* und die *Post* kritisieren, dass Ziffer 2.8.1 sehr rudimentär und minimalistisch formuliert sei. Sie geben zu bedenken, dass die Metadaten wohl gepflegt werden müssen und beantragen, dass die TOZ Vorgaben machen solle, wie die Gemeinschaften diese Anpassungen der Metadaten umsetzen müssen, hinsichtlich Geschwindigkeit, Vollständigkeit, etc.

2.9 Integrationsprofile (Abs. 3 Bst. d)

Die *FMH* verweist auch hier auf ihre Bemerkungen zu den entsprechenden Verordnungsartikeln. Die *SQS* fragt, ob es nur ein Bearbeitungsreglement der ZAS gebe. Ihre Suche nach einem Bearbeitungsreglement via zas.admin.ch sei erfolglos gewesen. Dies sei zu prüfen resp. genau zu bezeichnen. 6 Kantone[98] bemängeln, dass die Ziffer 2.9 technische Details enthalte, welche sich weiterentwickeln können und in dieser Form nicht in einen verbindlichen, rechtlichen Rahmen gehören würden. Die Ziffer sei zu vereinfachen und alle Verweise auf sich entwickelnde Normen zu streichen. Der Kanton *ZH* schliesst sich dieser Forderung an und betont, dass es nicht sinnvoll sei, in diesem Umfang technische Vorgaben zu machen. Gemäss der *medshare* könne nicht von sämtlichen Branchenteilnehmern verlangt werden, sich an alle Regulationen zu halten während die ZAS davon befreit sei. Sie schlägt vor, dass die ZAS IHE XCPD implementieren solle und die Gemeinschaften die elektronischen Patientendossier-PID mittels IHE XCPD bei der ZAS abfragen sollen.

2.9.1/2.9.2 Standardschnittstelle zur Identifikationsdatenbank der ZAS: Der *VAKA* warnt davor, dass zusätzliche Schnittstellen verwendet werden müssen. Die von *IHE* bereitgestellten Profile seien bereits anspruchsvoll in der Umsetzung. Analog der *K3* und dem *VZK* fordert er die Streichung von zusätzlichen Schnittstellen. Die *privatim* weisen darauf hin, dass nicht die Zugangspunkte der Gemeinschaften, sondern die Gemeinschaften selber dies sicherstellen müssten. Es solle eine Textanpassung vorgenommen werden, da die Zugangspunkte keine handlungspflichtigen Subjekte seien. 6 Kantone[99] schreiben, dass es unnötig sei, nochmals an die Tautologien zu erinnern. Dies zumal die Gemeinschaft beweisen müsse, dass sie über diese Vorgaben verfügt, aber nicht, dass sie diese einhaltet. Sie fordern die Streichung von Ziffer 2.9.2. Ebenfalls die Streichung dieser Ziffer fordern der *VAKA*, die *K3* und der *VZK*.

97 FR, NE, GE, VS, VD, JU
98 FR, NE, GE, VS, VD, JU
99 FR, NE, GE, VS, VD, JU

Sie fügen dazu an, dass solche Vorgaben zwingend im Rahmen der vorliegenden Verordnungen zu formulieren und nicht zu verschieben seien.

2.9.3 Integrationsprofile, nat. Anpassungen der Integrationsprofile und nat. Integrationsprofile: Die *BINT* und die *Integic* machen geltend, dass der entsprechende Nachweis für diese Konformität zu den genannten IHE-Profilen erforderlich sein müsse. Ohne Conformance Statements und Nachweis durch erfolgreich abgelegte IHE Connect-A-Thon-Tests sei dieses Kriterium nicht seriös zertifizierbar, womit diese für die relevanten IHE-Profile einzufordern seien. Die *Post* kritisiert, dass der Anwendungsbereich von Ziffer 2.9.3 nicht klar sei. Es sollte nur den Austausch zwischen Gemeinschaften und nicht innerhalb einer Gemeinschaft angewendet werden. Die Ziffer sei mit folgendem Zusatz zu ergänzen: „[…] Informationsübertragung zwischen Gemeinschaften die Integrationsprofile […]".

2.9.4 Akteure und Transaktionen der Integrationsprofile - Gemeinschaftsübergreifende Kommunikation: Die *BINT* und *HIN* sind der Meinung, dass die gemeinschaftsübergreifenden Zugriffe kostenlos ausgeführt werden müssen. Falls Gemeinschaften Roaming-Gebühren erheben dürfen, könne so die Ausbreitung und der föderative Ansatz des EPDG nicht umgesetzt werden. Es bestehe zudem die Gefahr von Monopolen, denn bereits das Patientenportal sei hinsichtlich des Betreibers eingeschränkt. Sie beantragen dementsprechend, dass Ziffer 2.9.4 folgendermassen ergänzt wird: „nach Anhang 5 der EPDV- EDI kostenlos unterstützen". Die *IG eHealth* und die *Post* geben zu bedenken, dass die Anforderung gemäss Ziffer 2.9.4.2 nicht nötig sein sollte. Ziffer 2.9.1 definiere die Schnittstelle zur ZAS. Die ZAS biete auch WebService an. Zudem weisen sie darauf hin, dass SEDEX nicht kostenlos sei und fragen, wer diese Kosten tragen solle. Sie schlagen die Löschung der Anforderung vor. Die *BINT*, die *Integic*, die *IG eHealth* und die *ahdis* sprechen sich für die Streichung von Ziffer 2.9.4.4 aus. Die Patient Location Query werde in Anhang 5 der EPDV-EDI explizit ausgeschlossen. Die *BINT*, die *Integic* und die *ahdis* plädieren zudem für die Aufnahme einer Ziffer 2.9.4.5; Update Document Set Cross Community [ITI-xxx]. Sie schreiben, dass es eine Cross Community Transaktion brauche, um die Dokument-Metadaten Vertraulichkeitsstufen in einer anderen Gemeinschaft zu ändern. Des Weiteren wünschen sie auch die Aufnahme einer Ziffer 2.9.4.6; On-Demand Documents Option (siehe ITI TF-2a, 3.18.4.1.2.5).

Die *SQS* gibt zu bedenken, dass im Rahmen von Audits eines Managementsystems technische Überprüfungen in dieser Tiefe nicht möglich seien und dem Verständnis von Audits (Stichprobe) widersprechen würden. Die hier beschriebenen Anforderungen seien zwingend zu erfüllende Abnahmekriterien, welche im Rahmen der Inbetriebnahmen von Systemen / Schnittstellen validiert und protokolliert werden müssen. Diese Abnahmen seien ausserhalb der eigentlichen Zertifizierung zu regeln, z.B. im Rahmen einer technischen Prüfung. Im Rahmen der Zertifizierung selber werde mittels Controls ausschliesslich überprüft, ob diese Prüfungen durchgeführt wurden und mögliche Befunde bearbeitet werden. Die Zertifizierungsnorm definiere hingegen nicht, wie schwerwiegend ein Befund ist. Konkret fordert die *SQS* die Ergänzung der Ziffern 2.9.4 – 2.9.21 mit einer Regelung bezüglich des Nachweises technischer Überprüfung der technischen Voraussetzungen. Diese Forderung wiederholt sie jeweils in sämtlichen relevanten Ziffern.

2.9.5/2.9.6 Akteure und Transaktionen der Integrationsprofile - Kommunikation beglaubigter Identitäten: Das *KSSG* schreibt bezüglich Ziffer 2.9.5, dass aus ihrer Sicht XUA dafür nicht ausreiche und XUA++ eingesetzt werden müsse. Die *ahdis* weist darauf hin, dass unter Ziffer 2.9.6 eine Ausführung fehle, wie der X-Service User die Assertion vom X-Assertion Provider bekommt und wie die Relation zum User Authentification Provider sein muss.

2.9.9 Akteure und Transaktionen der Integrationsprofile - Dokumente bereitstellen: Das *KSSG* fragt, ob es zwingend sei, dass die Dokumente mittels Provide and Register Document Set-b im Repository abgelegt werden. Es sei auch denkbar, dass die Dokumente über HL7 MDM im Repository abgelegt werden und dann mit der Transaktion Register Document Set in der Registry registriert werden. In St. Gallen sei dies so umgesetzt, da die Dokumenten-Quellen zum Teil kein Provide and Register Document Set-b unterstützen würden. Bei Medizinprodukten sei es eher unwahrscheinlich, dass diese Anforderung für

den Schweizer Markt entwickelt werde. Die Ziffer müsse insofern erweitert werden, dass auch andere Varianten zur Speicherung von Dokumenten im Repository zugelassen werden.

2.9.10 Akteure und Transaktionen der Integrationsprofile – Dokumenten-Metadaten mutieren: Die *IG eHealth* und die *Post* fragen, wer die Rolle „Document Administrator" übernehmen könne. Bei der Berücksichtigung von Autorenrechten wäre klar, dass jeder Autor implizit auch „Document Administrator" der von ihm publizierten Dokumente sei. Mit dem Wegfall von Autorenrechten könne das so nicht umgesetzt werden. Sie fügen an, dass Update und Delete Document starke Funktionen seien und es klar sein müsse, wer diese Funktionen ausüben darf. Sie bitten darum, dies zu definieren, falls nicht der Autor diese Funktion implizit erhalte. Die *IG eHealth* schreibt bezüglich Ziffer 2.9.10.1 zudem, dass gemäss Artikel 1 Absatz 1 EPDV immer eine Vertraulichkeitsstufe angegeben werden müsse. Des Weiteren wird die Streichung von Ziffer 2.9.10.2 empfohlen. Es reiche aus, die Metadaten zu ändern.

2.9.11 Akteure und Transaktionen der Integrationsprofile – Dokumentenregister: Die *IG eHealth* und die *Post* schreiben, dass das EPDG den Vertrauensraum zwischen den Gemeinschaften im Fokus habe. XDS.b Transaktionen seien „out of scope". Der Scope von dem EPDG, der EPDV und der TOZ sei klarer zu definieren. Die *Integic* weist bezüglich Ziffer 2.9.11.2 darauf hin, dass die korrekte Bezeichnung „Registry Stored Query" laute, was zu korrigieren sei. Zudem weist sie darauf hin, dass sich Inkonsistenzen in den angeführten Transaktionen finden liessen. Es seien teilweise Transaktionen angeführt, die Akteure ausführen bzw. empfangen/verarbeiten können müssen. Die Transaktionen, die je IHE Actor unterstützt werden müssen (also empfangen und senden) seien lückenhaft. Bspw. müsse 2.9.12. ITI-42 unterstützen, da diese Transaktion von Document Repository zu Document Registry erfolgt und nur bei Document Registry (2.9.11) angeführt sei. Diese Inkonsistenzen seien zu korrigieren.

2.9.12 Akteure und Transaktionen der Integrationsprofile – Dokumentenablage: Die *Integic* wiederholt einerseits ihre Stellungnahme von Ziffer 2.9.11, andererseits kritisiert sie, dass die für Clearing-Prozesse und zu Gunsten der Datenqualität in Verweisregistern essentielle Transaktion ITI-64 sowie das zugehörige IHE-Profil XAD-PID Change Management vollständig fehle. Die Transaktion ITI-64 sei zu ergänzen. Das *KSSG* wiederholt ihre Stellungnahme von Ziffer 2.9.9 bezüglich Ziffer 2.9.12.1.

2.9.15 Akteure und Transaktionen der Integrationsprofile - Patientenindex verwalten: Die *BINT* wiederholt ihren Kommentar von Ziffer 2.9.4 in Bezug auf Ziffer 2.9.15.3 und schlägt, genau wie die *Integic* und die *ahdis*, die Streichung dieser Ziffer vor. Eine Update Nachricht für die ID der Patientin / des Patienten sei nicht notwendig. Der Anwendungsfall sei nicht erkennbar.

2.9.16 - 2.9.18 Akteure und Transaktionen der Integrationsprofile - Authentisierung von Systemen und Protokollierung von IHE-Transaktionen: Die *Integic* und die *ahdis* fordern die Streichung des Textteils „grouped with Any IHE Actor" aus den Ziffern 2.9.16 und 2.9.17. Gemäss der *medshare* seien Secure Applications und Secure Nodes gleich zu behandeln. Die Unterpunkte von Ziffer 2.9.17 und Ziffer 2.9.18 müssten bei beiden Ziffern aufgeführt werden. Die *IG eHealth*, die *Integic* und die *ahdis* fordern die Ergänzung einer Ziffer 2.9.18.2 „Maintain Time [ITI-1]". Dies gemäss Anhang 5 EPDV-EDI, Punkt 1.4.2.4 ATNA Secure Application.

2.9.22 – 2.9.24 Authentisierung mit gültigen Zertifikaten: Die *OFAC* schreibt bezüglich elektronischen Zertifikaten aus den Zertifikatsdiensten gemäss ZertES, dass das ZertES die Voraussetzungen regle, unter denen sich Anbieter von Zertifikatsdiensten im Bereich der elektronischen Signatur anerkennen lassen können, auch bezüglich ihren Rechten und Pflichten. Es definiere den Rahmen, der natürlichen Personen erlaubt, Dokumente elektronisch zu unterzeichnen. Das ZertES sei aber auf den Bereich der elektronischen Signatur begrenzt und decke keinem Fall die Bedingungen über die Identifikation sowie die Authentifizierung der juristischen Personen und ihre verschiedenen technischen Zugangspunkte ab. Die Akquisitionsanforderung der Zertifikate bei den Anbietern der elektronischen Signaturdienste sei nicht fundiert und bringe keine zusätzliche Garantie für das elektronische Patientendossier gegenüber der Zertifizierungsstelle auf dem Markt. Die *Post* fragt bezüglich Ziffer 2.9.22, ob Softzertifikate gestattet seien. Die *medshare* macht geltend, dass die ZAS nicht anders behandelt werden solle als die zentralen

Abfragedienste. Sie schlägt die Vereinigung mit Ziffer 2.9.22.3 und auch in Artikel 38 Absatz 1 EPDV vor. Bei Ziffer 2.9.23 weist die *medshare* darauf hin, dass der Dokumentenverweis fehle. Des Weiteren wiederholt die *medshare* ihren Kommentar zu Ziffer 2.9 in Bezug zu Ziffer 2.9.24. CT (consistent time) sei eine Voraussetzung für ATNA. ATNA werde von den anderen IHE-Profilen vorausgesetzt. Sie schreiben, dass es mehr Sinn machen würde, dass CT die Schweizer Zeit als Quelle verwendet.

2.9.25 Konsistente Zeit der Schweiz: Die *SQS* fragt, wer wie bestimme, welche die relevanten informationsverarbeitenden Systeme sind. Sie wolle wissen, ob bspw. ein Smartphone oder ein Tablet ein relevantes System sei? Aussagen dieser Art würden zu unterschiedlicher Auslegung und Bewertung im Rahmen von Audits führen. Konkret wird gefordert, dass der Begriff „relevantes informationsverarbeitendes System" explizit beschrieben wird. Die *IG eHealth* und die *Post* fragen ihrerseits, weshalb hier nicht das Profil CT referenziert werde.

2.10 Protokolldaten (Abs. 3 Bst. e), Anforderungen an das Protokollierungssystem

Die *FMH* verweist auf ihre Bemerkungen zu den entsprechenden Verordnungsartikeln, insbesondere aber darauf, dass die Protokollierung der Zugriffe auch für die Behandelnden haftungsrechtliche Relevanz habe. Sie müsse zwingend dem Nachweis dienen, welche Daten ein Behandelnder zum Zeitpunkt eines Zugriffs gesehen hatte.

2.10.2: 7 Stellungnehmende[100] fragen, was „auf das erforderliche Mass" bedeute resp. wie dies definiert werde. Die *K3*, der *VZK*, der *ZAD* und der Kanton *ZH* fordern die Streichung dieser Bezeichnung. Der Kanton *ZH* fügt seiner Forderung hinzu, dass aus dem Protokoll auch – entgegen Ziffer 2.10.2 – erkennbar sein müsse, welche Daten abgerufen worden sind. Ansonsten sei die Patientin / der Patient nicht in der Lage zu beurteilen, ob der Zugriff rechtmässig erfolgte. Es sei darauf zu achten, dass das Protokoll unter allen Umständen vollständig ist. Nur so könne Vertrauen in das System geschaffen werden. Die *IG eHealth* wünscht die Aufnahme des Begriffes „erforderliches Mass" in die Begriffsdefinitionen. Andernfalls müsse das erforderliche Mass in einem Betriebsreglement national geregelt werden. Der Kanton *ZG* schlägt seinerseits die Präzisierung des Begriffs vor. Gemäss der *medshare* sei zudem der Begriff „medizinische Daten" unklar. Diese seien zu präzisieren.

2.10.3: Die *IG eHealth* und die *Post* fragen, ob es korrekt sei, dass es genüge, wenn eine nachträgliche Änderung nachgewiesen werden könne. Sie schlagen folgende alternative Formulierung von Ziffer 2.10.3.2 vor: „[…] von Protokolldaten muss klar erkennbar sein". Die *Tessaris* schreibt bezüglich der nachträglichen Veränderung von Protokolldaten, dass es sich in der Praxis ergeben könne, dass protokollierte Angaben unrichtig oder unvollständig sind. Es sollte somit möglich sein, Protokolldaten zu berichtigen oder zu ergänzen. Eine nachträgliche Veränderung von Protokolldaten dürfe nicht möglich sein. Ergänzungen, Berichtigungen oder Änderungen von Eintragungen im Protokoll seien als solche zu kennzeichnen und mit Angaben über Urheber und mit Zeitstempel zu versehen.

Bleuer macht bezüglich Ziffer 2.10.3.3 geltend, dass die Protokollierung der Einsichtnahme in die eigenen Daten ein Eingriff in die Privatsphäre der Bürgerin / des Bürgers sei und diese / dieser die Protokollierung ausdrücklich erlauben müsse. Gemäss dem Kanton *ZH* sei das elektronische Patientendossier so auszugestalten, dass Systemadministratoren keinen Zugriff auf die Patientendaten haben. Verschlüsselung und Schlüsselverwaltung seien so zu implementieren, dass weder die OS-Administratoren noch die DB-Administratoren die verschlüsselten Daten lesen können. Zu verschlüsseln seien dabei sämtliche Daten. Die *privatim* weisen betreffend den Ziffern 2.10.3.3 und 2.10.3.4 darauf hin, dass es für die Patientin / den Patienten auch sichtbar sein sollte, wenn Systemadministratoren auf Daten ihres elektronischen Patientendossiers zugegriffen haben. Sie fordern, dass die Regelung entsprechend angepasst wird.

Die *SQS* macht betreffend Ziffer 2.10.3.4 darauf aufmerksam, dass technische Einschränkungen mit entsprechenden Berechtigungen immer umgangen werden können. Somit müsse die Problematik auf

[100] IG eHealth, Integic, K3, VZK, ZG, ZH, ZAD

administrativem Weg gelöst werden. Die Beschränkung der Administratorenrechte sei in einer Weisung aufzunehmen. Ähnlich schreibt das *KSSG*, dass Protokolldaten bis zu deren Archivierung immer manipulierbar seien, weswegen die Regelung nur eingeschränkt umsetzbar sei. Ziffer 2.10.3.4 sei dementsprechend zu streichen oder anzupassen. *SCH* bemängelt ebenfalls die technische Umsetzbarkeit und schlägt folgende, alternative Ziffer 2.10.3.4 vor: „Systemlogs müssen revisionssicher aufbewahrt werden". Die *BFH* ist der Meinung, dass die Systemadministratoren auch keine anderen Aktivitäten löschen oder deaktivieren können sollten und fordern folgende Anpassung von Ziffer 2.10.3.4: „[…] die Protokollierung von Aktivitäten zu löschen oder zu deaktivieren".

2.10.4: Die *Integic* macht geltend, dass die unter Ziffer 2.10.4 aufgeführten Protokolleinträge ein Eingriff in die Privatsphäre der Bürgerinnen / Bürger darstellen, soweit sie die Einsichtnahme in die eigenen Daten betreffen. Die Patientin / der Patient müsse diesbezüglich entscheiden können. Ähnlich schreibt die *SUVA*, dass mit dieser Vorgabe die Privatsphäre der Patientin / des Patienten verletzt werde. Es müsse ihr / ihm freistehen, wann und wie sie / er auf ihre / seine Daten zugreife, ohne dass dies von einer Gesundheitsfachperson eingesehen werden kann. Hier müsse wohl im Einklang mit dem DSG eine andere Lösung gefunden werden. 6 Kantone[101] bemängeln die französische Übersetzung von Ziffer 2.10.4.1.3 und schlagen folgenden Wortlaut vor: „configuration des autorisations ou gestion des autorisations".

Die *Post* und die *IG eHealth* fragen bezüglich Ziffer 2.10.4.2, ob es sinnvoll sei, den Patientinnen / Patienten auch abgewiesene Zugriffsversuche im Log anzuzeigen. Sie bezweifelt, dass es wirklich nötig sei, jede Suche mit den entsprechenden Suchkriterien im Log anzuzeigen, da dies verwirrend sein könne, vor allem wenn nichts gefunden oder geliefert worden sei. Sie bitten um eine Präzisierung. Zu Ziffer 2.10.4.2.1 schreiben sie zudem, dass die Liste unter dem Fokus "Einsichtnahme durch Patient" stehe. Sie fragen, ob es korrekt sei, dass eine Patientin / ein Patient bei wahllosen Gesundheitsfachpersonen nachschauen könne, wann diese eingeloggt und ausgeloggt sind oder ob der Login/Logout der Patientin / des Patienten gemeint sei. Die Formulierung "Fokus" sei zu prüfen, die Protokollierung sei grundsätzlich sinnvoll. Sie schlagen zudem folgenden Zusatz vor: „die eigene Authentifizierung […]". Die *Post* bemängelt betreffend Ziffer 2.10.4.2.3, dass es sehr viele Einträge geben könne, vor allem da die Ärztinnen / Ärzte häufig unspezifisch suchen. Die Beschränkung der Anzahl Resultate in IHE-Profilen sei optional und es fehle eine Vorschrift, die dies zur MUSS-Anforderung mache. Die Informationsflut leiste keinen Beitrag zur Sicherheit. Die Formulierung der Ziffer sollte komplettiert und konsistent gemacht werden". Für *medshare* ist diese Ziffer unverständlich. Sie schreibt, dass nach Dokumenten, aber nicht nach dem elektronischen Patientendossier gesucht werden könne. Es solle präzisiert werden, was gemeint sei. Zu Ziffer 2.10.4.2.5 schreibt die *medshare* zudem, dass eine Präzisierung resp. Begründung zu erfolgen habe. Der *KSSG* weist darauf hin, dass die für die Patientin / den Patienten einsehbaren Logdaten durch das IHE ATNA Profil generiert werden. Ihrer Ansicht nach unterstütze das IHE ATNA Profil diese Anforderung nicht. Die Ziffer 2.10.4.2.7 sei zu streichen. Die Protokollierung eines neuen IDM könne in Systemlogs gefordert werden, jedoch nicht im ATNA. Somit sei es auch nicht für die Patientin / den Patienten einsehbar. *SCH* schreibt bezüglich Ziffer 2.10.4.2.7, dass die Registrierung eines neuen IDM ein Prozess sei, der isoliert im Identity Provider ablaufe. Der Identity Provider sei aber nicht zwingend eine IT-Komponente der Gemeinschaft, sondern könne an Dritte ausgelagert werden. Das SAML-Protokoll, welches für die Kommunikation der Portale mit den Identity Providern vorgeschrieben sei, sehe keinen Austausch von Protokoll-Daten zwischen dem Identity Provider und den Portalen vor. Die Information der Registrierung neuer IDM sei damit i.A. in der Gemeinschaft nicht verfügbar und könne dementsprechend auch nicht in den Protokollen registriert werden.

2.10.5: 6 Kantone[102] weisen darauf hin, dass solange sich das Resultat der Suche nicht nur auf eine einzige Patientin / einen einzigen Patienten beziehe, die Suche keine Historisierung brauche. Es sei zudem technisch unmöglich, einen Ausdruck zu tracken, oder einen Screenshot zu verhindern. Die Ziffern 2.10.5.1 bis 2.10.5.3 seien zu streichen. Die *Integic* wiederholt ihre Stellungnahme von Ziffer 2.10.4. Die *SUVA* macht darauf aufmerksam, dass ihre Bemerkungen unter 2.10.4 auch hier gelten, sofern es

[101] FR, NE, GE, VS, VD, JU
[102] FR, NE, GE, VS, VD, JU

sich um die Suche der Patientin / des Patienten in den eigenen Daten handle. Die *privatim* bemängelt, dass unklar sei, ob die Patientin / der Patient aus dem Protokoll sehen könne, wer auf ihre / seine Daten zugegriffen hat. Dies sei in jedem Fall eine wichtige Information und sollte aus dem Protokoll ersichtlich sein. In der Regel dürfte die zugreifende Person dem System bekannt sein. Ansonsten müsste das Protokoll einen Hinweis enthalten, die Zugriffe seien durch Unbekannt erfolgt. Es wird gewünscht, dass die Regelung entsprechend spezifiziert bzw. ergänzt werde. Gemäss der *SGMI* und der *FMH* gehe die Protokollierung der Suchfunktion resp. der Suchparameter zu weit. Dies sei zu streichen. Zugriffe gemäss create, read, update und delete würden geloggt. Die *BFH* kritisiert, dass bei Ziffer 2.10.5 von Mindestangaben die Rede sei, bei den Ziffern 2.10.5.1 – 2.10.5.3 aber Beispiele und „etc." angegeben werde. Es wird eine genaue Liste der Attribute, die mindestens in das Protokoll aufgenommen werden müssen, gefordert. Die *Post* fordert die Streichung von Ziffer 2.10.5.3, aufgrund fehlender Umsetzbarkeit.

2.10.6: Die *Tessaris* schlägt folgenden Zusatz für Ziffer 2.10.6 vor: „Die Protokolldaten sind 10 Jahre, und im Falle einer längeren Dauer der Aufbewahrung von Daten im elektronischen Patientenregister bis zur Löschung der betreffenden Daten, aufzubewahren". Gemäss der *privatim* sei aus Gründen der Klarheit festzuhalten, dass die Protokolldaten nach Ablauf der 10 Jahre zu vernichten sind. Eine dementsprechende Anpassung des Wortlauts sei zu prüfen.

2.11 Verknüpfung der PID mit Dokumenten (Abs. 3)

Die *OFAC* fragt, wie ein Dossier vollständig rekonstruiert werden könne, wenn die Verknüpfung der PID mit Dokumenten nicht gespeichert werden und weshalb die Verwendung der PID in Primärsystemen verboten sei. Die *privatim* verweisen an dieser Stelle auf ihre Ausführungen unter den allgemeinen Bemerkungen zur EPDV. Der Kanton *ZH*, die *K3* und der *VZK* schreiben, dass das Verbot, die PID nicht mit den Dokumenten zu verknüpfen nicht umsetzbar sei. Die Zuordnung eines internen Falls erfolge einmalig, danach müsse sichergestellt werden können, dass diese Zuordnung immer verwendet werden kann. Der Kanton *ZH* fügt an, dass eine Gemeinschaft nicht in der Lage sei sicherzustellen, dass die PID in den Primärsystemen nicht verwendet werde. Das Wort „persistent" solle mit „dauerhaft" ersetzt werden, was auch die *K3*, der *VZK* und *SBC* so sehen. Generell fordert der Kanton *ZH* aber, dass Ziffer 2.11.1 überarbeitet oder gestrichen wird. Die *SUVA* macht geltend, dass Gemeinschaften nicht die Verantwortung für die angeschlossenen Einrichtungen übernehmen können, weshalb Ziffer 2.11.1 zu streichen sei. *SBC* und die *BINT* fordern ebenfalls die Streichung. Die *BINT* schreibt dazu, dass die Gemeinschaften sicherstellen müssten, dass Primärsysteme ZAS-PID nicht genutzt werden. Dies sei durch Gemeinschaften jedoch nicht durchsetzbar. Des Weiteren schreibt sie, dass die Ziffer zu präzisieren sei und fragt, was in Verträge müsse, was durch wen kontrolliert werde und wie die Haftung sei. Aus der separaten Argumentation zur elektronischen Patientendossier-PID leite sich ausserdem die Notwendigkeit einer Vorgabe im umgedrehten Sinn ab: „Die PID ist in den Metadaten von Dokumenten persistent vorzuhalten", was auch die *Integic* und *Bleuer* so formulieren. Die Kantone *GE*, *FR*, *VS*, *VD* und *JU* weisen darauf hin, dass die Gemeinschaft nicht den Inhalt der Primärsysteme garantieren könne. Wenn eine Ärztin / ein Arzt eine PID mit medizinischen Dokumenten hält, entgehe dies der Kenntnis der Gemeinschaften. Sie könne hingegen Empfehlungen abgeben. Des Weiteren sei der Begriff „Dokumentenablage" nicht klar. Der MPI könne sich in derselben Dokumentenablage (data center) wie die Dokumente befinden, jedoch physisch von diesen getrennt. Ziffer 2.11.1 sei zu klären, aber nach dem Prinzip der Wirtschaftlichkeit gebe es keinen Vorteil daraus, eine PID zu generieren und diese nicht für die klare Identifizierung einer Patientin / eines Patienten nutzen zu können.

Gemäss der *IG eHealth* sei es zentral, dass Gemeinschaften sicherstellen müssen, dass die PID der ZAS nicht persistent in den Dokumentenablagen oder Dokumentenregistern gespeichert werde, was dem Erlasstext entspreche. Die Forderung, dass die PID in den Metadaten von Dokumenten persistent vorzuhalten sei, wird entschieden abgelehnt. Wird die PID auf allen Dokumenten vermerkt, gingen im Fall eines gewollten oder nötigen Nummernwechsels sämtliche Beziehungen verloren, d.h. Dokumente können bei einem Wechsel der PID nicht mehr eindeutig einer Patientin / einem Patienten zugeordnet werden. Dies sei aus Sicht des Datenschutzes problematisch. Das Konzept, Dokumente über den MPI

und lokale Schlüssel zu verbinden, sei zwar komplexer, aber erlaube die separate Bearbeitung von Dokumenten. Dies deshalb, weil auf jedem Dokument der Name und das Geburtsdatum der Patientin / des Patienten vermerkt sei. *HIN* kritisiert, dass vor allem der zweite Teil von Ziffer 2.11.1 technisch unmöglich durchsetzbar sei. Letztlich könne man via Zwischenablage / Screenshots die Nummer kopieren und ins Primärsystem anfügen. Es sei auch der scheinbare Widerspruch zur Figur 2 in Anhang 5, Nationale Anpassungen der Integrationsprofile, zu beachten. *HIN* fordert die explizite Erwähnung, dass diese Anforderungen vor allem organisatorisch zu lösen seien.

3. Zugangsportal für Gesundheitsfachpersonen (Art. 10 EPDV)

6 Kantone[103] schreiben, dass der Detaillierungsgrad in Ziffer 3 mehr funktionalen Spezifikationen („wie") entspreche als Anforderungen, die ihren Platz in Verordnungen hätten („was").

3.1 Konformität mit gesetzlichen Bestimmungen

Der *ZAD*, die *K3*, der *VZK* sowie die Kantone *ZH* und *ZG* schreiben, dass das Zugangsportal den TOZ zu entsprechen habe. In den TOZ könne nicht verlangt werden, dass es «den einschlägigen rechtlichen Anforderungen» zu entsprechen habe, da dies ohnehin gelte. Zudem sei keine Zertifizierungsstelle in der Lage zu bestätigen, dass das Zugangsportal alle rechtlichen Anforderungen einhalte. Der *VAKA* bezeichnet die Vorgabe gemäss Ziffer 3.1.1 als deklaratorisch. Zudem ertöne es etwas hilflos. 7 Stellungnehmende[104] fordern die Streichung von Ziffer 3.1.1, wobei für die *medshare* auch eine namentliche Aufführung der Anforderungen denkbar wäre. Gemäss der *privatim* sei es unklar, was mit dieser Regelung bezweckt werde. Wenn eine solche Regelung Sinn machen solle, müsse ausgeführt werden, welchen einschlägigen rechtlichen Anforderungen das Zugangsportal insbesondere (keine abschliessende Aufzählung) zu genügen habe.

3.2 Darstellung

Für die *K3*, den *VZK*, den *ZAD* sowie die Kantone *ZH* und *ZG* erscheinen die Bestimmungen gemäss Ziffer 3.2 als nicht erforderlich, weshalb sie zu streichen seien. 8 Stellungnehmende[105] machen darauf aufmerksam, dass bei Ziffer 3.2.1.1 das Wort „Gesundheitsfachperson" vergessen ging, womit es nachzutragen sei: „ob ein Dokument durch eine Gesundheitsfachperson oder durch […]". Die *SQS* weist ebenfalls darauf hin, dass der betreffende Satz nicht vollständig sei, was zu beheben ist.

Der *VAKA* fragt, wie man sich die Forderung gemäss Ziffer 3.2.1.2, insbesondere auch im Kontext von Hilfspersonen, vorzustellen habe und ob diese im Namen der primären / übergeordneten Gesundheitsfachperson agieren würden. Dieser Sachverhalt sei mit genauen Erläuterungen zu klären. Ähnlich fragt die *Post*, wie die eigens publizierten Daten gekennzeichnet sein müssen und ob die Angabe des Autors genüge. Hier dränge sich die Frage auf, wie "selbst" zu interpretieren sei, wenn Hilfspersonen, oder andere Mitglieder der gleichen Gruppe involviert sind. Dies sei zu konkretisieren, Hilfspersonen sollen im Namen der Ärztin / des Arztes agieren.

Die *GDK* und 9 Kantone[106] machen im Zuge von Ziffer 3.2.1.3 darauf aufmerksam, dass im Ausführungsrecht und dessen Erläuterungen die Begriffe bzw. Konzepte der „Vernichtung", „Löschung" und „Annullierung" in Bezug auf Daten des elektronischen Patientendossiers auftauchen. Es stelle sich die Frage, wie diese Konzepte technisch zu unterscheiden seien. Die *GDK* und 8 Kantone[107] regen an, dass die Konzepte in den Erläuterungen auszuführen und voneinander abzugrenzen seien, sodass sie konsistent angewendet werden können. Ausserdem müsse auch der Patientin / dem Patienten klar sein,

[103] FR, NE, GE, VS, VD, JU
[104] ZG, ZH, ZAD, K3, VZK, VAKA, medshare
[105] KKA, BüAeV, GAeSO, KAeG SG, HIN, Medgate, privatim, pharmaSuisse
[106] BL, GL, LU, OW, UR, FR, NW, SZ, TG
[107] BL, GL, LU, OW, UR, FR, NW, SZ

inwiefern sich z.B. ein annulliertes Dokument von einem gelöschten unterscheidet. Die *SBC* fragt ihrerseits ebenfalls, was „annuliert" bedeute und wünscht diesbezüglich eine Erklärung. Gemäss der *Post* sei zu klären, ob annullierte Dokumente den Patientinnen / Patienten überhaupt angezeigt werden müssen resp. ob es nicht genüge, die Löschung in der History / Log anzuzeigen.

Der *VGIch* schreibt bezüglich den Ziffern 3.2.1.3 und 3.2.1.4, dass pro Dokument eine Versionierung sicherzustellen sei und zusätzlich von „gültigen" und „annullierten" Dokumenten gesprochen werde. Zudem könne ein Dokument gemäss den „Metadaten" einen Verfügbarkeitsstatus „genehmigt" und „abgelehnt" aufweisen. Die Terminologie sollte zum besseren Verständnis geklärt und ggf. vereinheitlicht werden. Der *VAKA* gibt betreffend Ziffer 3.2.1.4 zu bedenken, dass eine Versionierung, sofern überhaupt, in Anwendung meist nur verwirrend sei und fragt, ob dies gegenüber den Patientinnen / Patienten kaum verfügbar gemacht werden solle. Es wird vorgeschlagen, dass in Richtung Patientin / Patient nur die aktuellste Version verfügbar gemacht wird. Ähnlich fragt die *Post*, ob es nicht benutzerfreundlicher sei, der Patientin / dem Patienten einfach die letzte, aktuellste Version anzuzeigen, was sie gleichzeitig vorschlägt.

3.3 Barrierefreiheit

Der *VAKA* begrüsst zwar Barrierefreiheit sehr, da diese aber bereits kostenintensiv in der Umsetzung sei, verteure es die Umsetzung weiter, wenn sie auch noch zertifiziert werden müsse. Gemeinschaften und Stammgemeinschaften würden in jedem Fall vorsehen, dass Zugangsportale barrierefrei gestaltet werden. Die dazugehörige Vorgabe in der TOZ sei zu streichen. Gemäss dem *KSSG* werde mit diesem Artikel gefordert, dass das Zugangsportal und damit verbunden auch die Integration in den Primärsystemen barrierefrei sein müssen. Implizit würde dies bedeuten, dass z.B. das komplette KIS barrierefrei zu sein habe. Es wird die Streichung von Ziffer 3.3 im Zusammenhang mit dem Zugangsportal für Gesundheitsfachpersonen gefordert. Der *SBV* bemängelt, dass lediglich auf barrierefreies Web eingegangen werde und fragt, wie es mit Apps aussehe und ob diese im Dokument berücksichtigt werden. Es müsste auch hier die Anforderung an die Barrierefreiheit definiert werden. Die Kantone *ZG* und *ZH* erachten die Bestimmungen zudem als nicht erforderlich und wünschen ebenfalls deren Streichung. Die Kantone *GE*, *VS*, *VD*, *JU* und *NE* machen darauf aufmerksam, dass es ältere Gesundheitsfachpersonen gebe, welche sich gut mit Informatik auskennen, während jüngere Ärztinnen / Ärzte starke Vorbehalte gegenüber der Nutzung dieser Tools haben. Zudem fragen sie, um welche Behinderungen es sich handle, Sehprobleme oder psychische Behinderungen? Sie fordern, dass Ziffer 3.3.1.1 gestrichen wird. 6 Kantone[108] schreiben zudem bezüglich Ziffer 3.3.1.2, dass sich dieser Entscheid auf eine Norm beziehe, die sich entwickeln könne und die keinen Platz in dieser Form in einer Gesetzgebung bekommen soll. Während die Kantone *GE*, *VS*, *VD*, *JU* und *NE* die Streichung fordern, spricht sich der Kanton *FR* für eine Vereinfachung aus. Die *SQS* wiederholt bezüglich Ziffer 3.3.1.2 ihre Bemerkung von Ziffer 2.9.4 und fordert deren Ergänzung mit einer Regelung bezüglich eines Nachweises technischer Überprüfung der technischen Voraussetzungen. Gemäss dem *SBV* sei die Konformitätsstufe AA gemäss Ziffer 3.3.1.2 für Menschen mit Sehbehinderungen unzureichend. Die Konformitätsbedingungen gemäss WCAG 2.0 solle entsprochen werden und die Konformitätsstufe AAA erreicht werden.

3.4 Dateiformate: Bereitstellung

Für die *K3*, den *VZK*, den *ZAD* sowie die Kantone *ZG* und *ZH* erscheinen die Bestimmungen gemäss Ziffer 3.4 als nicht erforderlich, womit sie zu streichen seien. *SCH* schreibt, dass es a priori nicht bekannt sei, welche Formate die Patientin / der Patient oder der Leistungserbringer über das Portal im elektronischen Patientendossier speichern wolle. Insbesondere könne nicht ausgeschlossen werden, dass die Patientin / der Patient oder Leistungserbringer proprietäre Formate nutzen wolle, für die keine Programme zur Konvertierung oder nur Programme mit unvollständiger Konvertierung verfügbar sind. Zudem stelle eine Konvertierung in eines der erlaubten Formate eine Datenbearbeitung im Sinne des DSG dar. *Bleuer* schreibt, dass Anhang 4 (und nicht 3) die Austauschformate definiere, was im Text von Ziffer 3.4.1.1 dementsprechend anzupassen sei.

[108] FR, NE, GE, VS, VD, JU

Gemäss 6 Kantonen[109] ist es aus Gründen der Datenintegration gefährlich, dass das Portal eine Quelldatei umwandelt. Es sei die Verantwortung der Gesundheitsfachpersonen für das richtige Format zu sorgen. Zudem fragen sie, ob dies bedeute, dass das Zugangsportal in der Lage sein müsse, mehrere Formate lesen zu können. Sie fordern die Streichung von Ziffer 3.4.1.2. *Bleuer* weist darauf hin, dass bei Umwandlungen sinnentstellende Fehler auftreten können. Deshalb müssten die Originalformate zusätzlich vorgehalten werden. Mit dem Vorhalten im Originalformat werde eine Einschränkung auf zugelassene Formate problematisch. Auf jeden Fall sollte die Zulassung die allgemein üblichen Formate zulassen, darunter insbesondere auch ZIP und ISO. Er wünscht folgende Formulierung von Ziffer 3.4.1.2: „[…] in eines der in Anhang 4 aufgeführten Formate umwandeln. Dokumente sind bei Umwandlung zusätzlich im Originalformat vorzuhalten". Ähnlich schreiben die *BINT* und die *Integic*, dass bei Umwandlungen Dateien auch im Originalformat abzulegen seien. Das bedeute eine Zulassung von Objekten auch als Bitstream. Die *SUVA* gibt zu bedenken, dass eine Umwandlung nicht mit der Revisionssicherheit vereinbar sei und spricht sich für die Belassung der Dateien im Originalformat aus. Die *Post* fragt, wieso auch gängige Dokumententypen umgewandelt werden müssen und wer die Verantwortung übernehme, falls bei der automatischen Umwandlung Informationen verloren gingen, was zu einer falschen Behandlung führe. Die *K3* und der *VZK* plädieren dafür, dass die Umwandlung beim Upload nicht zulässig sein dürfe. Bei der Umwandlung könnte der Inhalt verfälscht werden und die Datenintegrität wäre verletzt. Das Resultat würde ausserhalb der Kontrolle des Autors liegen und das Dokument könnte somit eine andere Aussage erhalten. Die Regelung sei so anzupassen, dass eine Umwandlung beim Upload nicht zulässig ist. Es sollten keine Dokumente umgewandelt werden dürfen, weswegen die Anforderung zu streichen sei. Die *Integic* fügt zu Ziffer 3.4.1.2 die Fragen an, welche Konvertierungswege vorgesehen seien und wie mit dem Upload von Daten von Fitnesstrackern oder Apps umzugehen sei. Für *HIN* müsse es im Interesse der Primärsystemhersteller liegen, die entsprechenden Konvertierungen anzubieten. Der Ansatz solle sein, dass das Portal nur gewisse Dateitypen zulässt. Es wird folgende Neuformulierung von Ziffer 3.4.1.2 gefordert: „Dateien der im Anhang 3 definierten Formate entgegennehmen. Dateien in anderen Formaten müssen entweder automatisiert umgewandelt oder abgewiesen werden". Die *medshare* wünscht folgenden, präzisierenden Zusatz zu Ziffer 3.4.1.2: „[…] in ein gemäss 3.4.1.1 zugelassenes Format umwandeln".

3.5 Dateiformate: Abruf

Für die *K3*, den *VZK*, den *ZAD* sowie die Kantone *ZG* und *ZH* erscheinen die Bestimmungen gemäss Ziffer 3.5 als nicht erforderlich, womit sie zu streichen seien. Die *Post* fragt, weshalb gängige Dokumenttypen, wie Word, nicht unterstützt werden.

3.5.1: Die *privatim* verweisen betreffend Ziffer 3.5.1.2 auf ihre Ausführungen unter den allgemeinen Bemerkungen zu der EPDV. *SBC* weist darauf hin, dass „bulk download" eine Sicherheitslücke erlaube, weshalb Ziffer 3.5.1.3 zu streichen sei. Die *Integic* fragt, ob bei einem „bulk download" je Dokument eine entsprechende Verifikation durch den Benutzenden einzugeben sei, oder einmal gesammelt werde. Dies sei klarzustellen resp. zu ergänzen. Betreffend Ziffer 3.5.1.5 weisen die *BINT*, die *Integic* und die *IG eHealth* darauf hin, dass „menschenlesbar" nicht ein Problem des Herunterladens, sondern der Darstellung sei. Es stelle sich die Frage, ob ein serverseitiges Rendering gemeint sei. Falls ja, müsste das ausformuliert werden. Die *SUVA* wünscht ihrerseits die Präzisierung, was unter „menschenlesbar" zu verstehen sei. Gemäss dem *KSSG* könne nicht davon ausgegangen werden, dass das Zugangsportal mit jeder Art von strukturierten Daten umgehen kann, sondern nur mit den im EPDV-EDI Anhang 4 aufgeführten Austauschformaten. Die Ziffer 3.5.1.5 sei damit soweit zu ergänzen, dass diese nur für die in EPDV-EDI Anhang 4 aufgeführten Austauschformate gilt. 6 Kantone[110] fordern die Streichung von Ziffer 3.5.1.1 und die folgenden Umformulierungen bei den Ziffern, 3.5.1.2, 3.5.1.3 und 3.5.1.5: „ 3.5.1.2 permettre d'enregistrer des fichiers présents dans le système primaire ("upload"); 3.5.1.3 prévoir la publication, non seulement un par un, mais aussi en masse ("bulk upload") des documents sélectionnés; 3.5.1.5 […] données structurées brutes ou d'exporter la forme affichée de ces données". Die *OFAC*

[109] FR, NE, GE, VS, VD, JU
[110] FR, NE, GE, VS, VD, JU

weist bezüglich dem „bulk download“ in Ziffer 3.5.1.3 darauf hin, dass in diesem Fall eine wichtige Datenmenge über die Patientin / den Patienten den Gemeinschaften und der Kontrolle entgehen würde. Diese Bestimmung stehe zudem im Widerspruch mit dem Konzept „Patient Empowerment“.

3.5.2: Die *medshare* macht darauf aufmerksam, dass beim Wort „erlaubte“ im Text ein Schreibfehler vorliege. Die *K3* und der *VZK* kritisieren, dass die Formulierung ungenau sei und einer Präzisierung bedürfe. Ähnlich fragt die *SQS*, wer zulässige Obergrenzen definiere und verlangt, dass die Zuständigkeit für die Definition der zulässigen Obergrenzen präzisiert wird. Gemäss der *Integic*, der *BINT* und der *IG eHealth* sei ein absolutes Limit nicht zulässig. Weitere verfügbare Dokumente müssten erkannt und einfach abgerufen werden können. Für die *Post* ist die Argumentation für rate limits nicht nachvollziehbar. Die Patientin / der Patient habe entschieden, dass die zugreifende Gesundheitsfachperson Zugriff auf das elektronischen Patientendossier habe. Ein künstlicher Riegel scheine nicht angemessen. Gemäss *Bleuer* bestehe die Gefahr, dass die Dokumente unvollständig abgerufen werden. Ziffer 3.5.2 sei zu streichen. Die *SUVA* spricht sich ebenfalls für die Streichung aus und weist darauf hin, dass die Bestimmung zu unvollständigen Daten der Patientin / des Patienten führen würden. Bei den eigens durch die Patientin / den Patienten hinzugefügten Daten könne dies zu einem Eingriff in ihre / seine Privatsphäre führen, da sie / er nicht die Möglichkeit habe, die gewünschten Daten zu übertragen. *HIN* geht davon aus, dass die rate limits von den Gemeinschaften definiert werden dürfen und sollen. Ziffer 3.5.2 sei folgendermassen zu ergänzen: „[…] auslösen. Die rate limits werden von den Gemeinschaften definiert“.

4. Datenschutz und Datensicherheit (Art. 11 EDPV)

Die *ISSS* fordert eine neue Ziffer 4.25 damit sichergestellt sei, dass Patientendaten nicht nach deren Vernichtung in alle Ewigkeit in Datensicherungen fortbestehen. Folgender Text wird gewünscht: „4.25 Datensicherung (Backups): Datensicherungen sind spätestens nach 2 Jahren zu vernichten, sofern keine gesetzlichen oder regulatorischen Anforderungen etwas Anderes verlangen. Im Falle belegbarer, betrieblicher Notwendigkeit kann diese Dauer auf maximal 3 Jahre ausgedehnt werden“. Die *SQS* weist darauf hin, dass durch die ganze Ziffer 4 ein Grossteil der ISO/IEC 27001:2013 Normteile und der Controls des Anhangs A zu finden sei. Es wäre sinnvoller auf die ISO/IEC 27001:2013 inkl. Anhang A zu verweisen und nur die EPDV spezifischen Zusätze zu beschreiben. Ein solcher Zusatz wäre bspw. die Meldung sicherheitsrelevanter Vorfälle an das BAG. Im Anhang werden zudem Begriffe benutzt, die der ISO/IEC 27001:2013 nicht entsprechen. Konkret wird die Separierung der Elemente ISO/IEC 27001:2013 Normteile und der Controls des Anhangs A von den EPDV spezifischen Zusätzen vorgeschlagen und die Einsetzung der Begriffsterminologie der ISO/IEC 27001:2013 gefordert. Die *FMH* weist darauf hin, dass man sich bezüglich Regelungen zum Datenschutz an den bestehenden Normen und good practice orientieren solle, und keine neuen Regelungen zu erstellen seien. Analog der *SGMI* fordert die *FMH* die Überarbeitung der ganzen Ziffer 4. Gemäss der *Tessaris* ist davon auszugehen, dass die umfangreichen organisatorischen und technischen Anforderungen aus Ziffer 4 durch eine Gemeinschaft mit beschränkten personellen und materiellen Ressourcen, wie eine einzelne Arztpraxis oder eine kleinere Gemeinschaftspraxis, welche das elektronische Patientendossier einführen und betreiben möchte, nicht eigenständig bewältigt werden können, sondern dafür Dritte (“Betriebsorganisationen“) beigezogen werden müssen. Wenn solche Betriebsorganisationen Dienste für Gemeinschaften erbringen, sollten sie grundsätzlich auch die Anforderungen aus Artikel 11 EPDV und Ziffer 4 erfüllen, da sonst eine Lücke im Dispositiv zur Gewährleistung von Datenschutz und Datensicherheit entstehe.

4.1 Anforderungen an Dritte

Die *privatim* schreiben, dass diese Regelung aus datenschutzrechtlicher Sicht zu begrüssen sei. Obwohl sich diese bereits aus dem Bundes- und den kantonalen DSG ergebe, erscheine es im Sinne der Klarheit und Vollständigkeit sinnvoll, diese in die TOZ aufzunehmen.

4.2 Datenschutz- und Datensicherheitsverantwortlicher (Abs. 1)

4.2.1: *HIN* begrüsst, dass die Norm ISO 27001 explizit erwähnt sei. Die *SQS* macht darauf aufmerksam, dass die ISO/IEC 27001:2013 kein Datenschutz- und Datensicherheitsmanagementsystem, sondern ein ISMS beschreibe. Das zu betreibende Datenschutzmanagementsystem müsse auf der Norm ISO/IEC 27001 aufbauen bzw. die Norm ISO/IEC 27001 erfüllen. Geeignet für die Beschreibung des Datenschutzmanagementsystems seien hingegen die „Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 14. Juni 2014" des EDÖB, welche bei einer Zertifizierung nach Artikel 11 DSG zur Anwendung gelangen. Die *SQS* schlägt die folgenden beiden Varianten für die Formulierung von Ziffer 4.2.1 vor: „Gemeinschaften müssen ein Informations- und Managementsystem betreiben, wie in der Norm ISO/IEC 27001:2013 beschrieben wird, das: […]" und „Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben, wie in den Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Richtlinien über die Zertifizierung von Organisation und Verfahren) vom 14. Juni 2014 des EDÖB beschrieben wird, das: […]". Die Kantone *ZH* und *ZG*, der *ZAD*, die *K3* und der *VZK* erachten Ziffer 4.2.1 als nicht sinnvoll und wünschen daher die Streichung. Die *OFAC* schreibt, dass die Datenschutz- und Datensicherheitsmanagementsysteme perfekt gemeinsam funktionieren würden, aber niemals verwechselt werden sollten. Die beiden Systeme sollten getrennt verwaltet werden. Zudem weist sie, ähnlich wie die *SQS*, darauf hin, dass die Norm ISO/IEC 27001:2013 keine Datenschutzmanagementsysteme definiere, womit der Satz neu zu formulieren sei.

4.2.2 / 4.2.3: Die *ISSS* schreibt, dass via den Ziffern 4.2.2.3.1 – 4.2.2.3.3 und 4.2.2.3.5 bewusst auch die Komponenten für die ICT-Fachdisziplinen wie Angriffssicherheit, Betriebsausfallsicherheit und System- und Daten-Backup abverlangt werden sollten. Dies zur Awareness und Grundlage für Management Review / Auditierungen / Zertifizierungen. Sie schlagen für die erwähnten Ziffern folgende Zusätze vor: Ziffer 4.2.2.3.1: „Hardware (Inventar der Datenspeicher, Server, Backup-Systeme, Sicherheitsfunktionen); Ziffer 4.2.2.3.2: Software (Inventar von Betriebs- und EPD-Anwendungssystem, Endpoint Protection, Backup, Monitoring, Update- und Patch-Management); Ziffer 4.2.2.3.3: Datenbestände (Beschreibung zu Datenhaltung, Datenorganisation, Datensicherheit, Berechtigungen); Ziffer 4.2.2.3.5: Prozesse (zu Datenschutz- und Datensicherheitsmanagementsystem, insbesondere auch zu Ausfallszenarien, Recovery, Tests, Audits, Verantwortlichkeiten). Die *Post* fragt bezüglich Ziffer 4.2.2.3, ob das Inventar alle angeschlossenen Primärsysteme einschliesse oder ob es hier lediglich um die zentralen Komponenten gehe. Sie beantragt, dass der Scope der TOZ klar umschrieben wird. Die *SQS* bemängelt, dass die Bestimmungen gemäss den Ziffern 4.2.2 und 4.2.3 nicht kongruent mit denjenigen des Artikels 11 EPDV seien. Entweder sei Artikel 11 EPDV zu ergänzen oder die beiden Ziffern anzupassen. Bezüglich Ziffer 4.2.2.3 schreibt die *SQS*, dass das Inventar in ISO/IEC 27001:2013 nicht nur Betriebsmittel betreffe. Die Norm spreche von Assets / Werten der Organisation. Dazu gehörten bspw. auch die Mitarbeitenden. Die Aufbauorganisation sei zudem zu wenig umfassend. Es wird folgender Text vorgeschlagen: „Ein aktuelles Inventar der folgenden Werte der Organisation". Entsprechend sei auch Ziffer 4.2.3 folgendermassen anzupassen: „[…] an den Werten der Organisation sind zu […]".

4.3 Datenschutz und Datensicherheitsverantwortlicher (Abs. 1 Bst. a)

20 Stellungnehmende[111] sind der Ansicht, dass auf die Schaffung von besonderen „Datenschutz- und Datensicherheitsverantwortlichen" zu verzichten sei. 14 Stellungnehmende[112] fügen hinzu, dass der Sicherheitsgewinn durch solche Verantwortliche nicht ersichtlich sei. Zudem seien die Kosten für die Einrichtung solcher Stellen hoch. Der *ZAD*, die *GDK* und 8 Kantone[113] weisen darauf hin, dass die TOZ hier von den Erläuterungen zu Artikel 11 EPDV abweichen würden, in welchem von einer „fachlichen und organisatorischen" Unabhängigkeit des Datenschutzverantwortlichen die Rede sei. Der Kanton *AR* ist der Meinung, dass der zuständige Datenschutzbeauftragte, bei genügender Kapazität, diese Aufgabe übernehmen sollte und in diesem Fall auf die Einsetzung einer unabhängigen Stelle verzichtet

[111] NW, TI, FR, ZG, K3, VZK, SGMI, FMH, BL, GDK, GL, LU, OW, UR, SZ, ZH, ZAD, ZG, K3, VZK
[112] NW, TI, FR, ZG, K3, VZK, BL, GDK, LU, OW, UR, SZ, ZH, ZAD
[113] BL, GL, LU, OW, UR, SZ, ZH, TG

werden könne. 6 Stellungnehmende[114] fordern explizit die Streichung von Ziffer 4.3.

Gemäss dem Kanton *SZ* sei es bezüglich Ziffer 4.3.1.1 nicht sinnvoll zu verlangen, dass die Datenschutzverantwortlichen ihre Funktion unabhängig ausüben können. Analog der *K3*, dem *VZK*, dem Kanton *ZG* und dem *ZAD* fragt der Kanton *SZ* zudem, was genau damit gemeint sei. Für die *privatim* wäre es wünschenswert, wenn unter der Ziffer 4.3.1 ein weiterer Punkt festgehalten würde, welcher besagt, dass der Datenschutzbeauftragte über die für die Aufgabe erforderlichen Fachkenntnisse verfügen muss. Zudem sei bei Ziffer 4.3.1.2 mit Blick auf die Ressourcen zu präzisieren, dass sowohl die zeitlichen als auch die finanziellen Ressourcen gemeint sind. Der *VGIch* bezeichnet Ziffer 4.3.1.2 als zu unspezifisch und fordert eine Präzisierung mittels klaren Kriterien. Des Weiteren wünscht die *medshare* folgenden Zusatz zu der Ziffer: „[…] erforderlichen Ressourcen und Entscheidungskompetenzen verfügt“ und der Kanton *BS* würde folgende Formulierung bevorzugen: „[…] erforderlichen Kompetenzen und Ressourcen verfügt“.

4.4 Erkennen von Sicherheitsvorfällen (SIEM) (Abs. 1 Bst. b)

Das *KSSG* gibt zu bedenken, dass der Aufbau von einem SIEM sehr aufwändig sei und sich kaum innerhalb der Übergangsfrist von 3 Jahren implementieren lasse. Ziffer 4.4 sei zu lockern oder die Fristen für deren Umsetzung zu verlängern. Gemäss dem *VGIch* darf sich das SIEM nur auf die technischen und organisatorischen Teile der Gemeinschaftsinfrastruktur beschränken, welche der Bereitstellung des elektronischen Patientendossiers dienen, nicht aber auf (logisch getrennte) Erweiterungen zur Bereitstellung gerichteter Kommunikation und nicht auf die Infrastruktur und Organisation der angeschlossenen Institutionen angewendet werden. 6 Kantone[115] schreiben, dass ein SIEM nicht auf Primärsysteme der Gesundheitsfachpersonen angewendet werden könne und wünschen dementsprechend folgenden Zusatz zu Ziffer 4.4.1.1: „[…] de la communauté à l’exclusion des système primaires, qui détecte […]“. Gemäss der *ISSS* sei im Hinblick auf die praktische Umsetzung vorzusehen, dass die beauftragten Personen eine Schulung, Kurs oder Attest absolvieren müssten. Ziffer 4.4.1.3 sei deshalb folgendermassen zu ergänzen: „[…] adressiert werden. Speziell sind mittels Sensibilisierungsmassnahmen, Schulungen oder Erfahrungsaustausch mit anderen Verantwortlichen die beauftragten Personen innerhalb der Gemeinschaft angemessen und wiederkehrend zu unterstützen“.

Die *Post* kritisiert, dass Ziffer 4.4.2.2 schwammig formuliert sei. Die Beurteilung, was unüblich sei und wie unüblich erkannt werden könne, sei sowohl für die Gemeinschaft wie auch für den Auditor schwierig umzusetzen. Des Weiteren sei unklar, was eine kritische Mutation nach Ziffer 4.4.2.3 sei. Die beiden Ziffern seien zu konkretisieren.

4.5 Umgang mit Sicherheitsvorfällen (SIEM) (Abs. 1 Bst. b)

Der *VAKA*, die *K3* und der *VZK* fragen, was ein formales von einem normalen Verfahren unterscheidet. Die *medshare* ist der Meinung, dass bei Ziffer 4.5.1.1 der Dokumentverweis zur EPDV fehle, was zu ergänzen sei. Die *FMH* und die *SGMI* sprechen sich für eine Präzisierung von Ziffer 4.5.1.1 aus. Es mache kaum Sinn alles zu melden. Die *Post* vermisst an dieser Stelle eine klare Umschreibung des Scopes, was zu beheben sei. Die *ISSS* fordert folgende Umformulierung von Ziffer 4.5.1.1 aufgrund der Konformität zur EU-Datenschutzgrundverordnung (EU-DSGVO): „formale Verfahren für das Melden von Datenschutz- und Datensicherheitsereignissen an die betroffenen Patientinnen / Patienten gemäss Ziffer 4.13 definiert haben“. Die *SQS* macht geltend, dass es nicht Funktion und Aufgabe einer Zertifizierungsstelle sei, Meldungen von Datenschutz- und Datensicherheitsereignisse zu empfangen und die Behebung zu kontrollieren. Die Zertifizierungsstelle als Eskalationsstelle sei aus Ziffer 4.5.1.1 zu streichen. Die *medshare* wünscht, dass Ziffer 4.5.2.2.1 folgendermassen präzisiert wird: „[…] Sperren des Zugangspunktes und Zugangsportals der Gemeinschaft […]“.

[114] ZH, K3, VZK, ZG, TI, NW
[115] FR, NE, GE, VS, VD, JU

4.6 Schutz vor Schadcode (Abs. 1 Bst. b)

Der *ZAD* sowie die Kantone *NW*, *TI* und *ZH* kritisieren, dass die Regelung gemäss Ziffer 4.6 zu detailliert sei. Sie sei zu streichen und es wäre zielführender, dazu generell-abstrakte Grundsätze in der EPDV aufzustellen. Die *Post* wiederholt bezüglich Ziffer 4.6.1.1 ihre Forderung von Ziffer 4.5.1.1.

4.7 Umgang mit Sicherheitsschwachstellen (Abs. 1 Bst. b)

Die Kantone *NW* und *ZH* sowie der *ZAD* wiederholen ihre Stellungnahme von Ziffer 4.6. Der *ZAD* schlägt im Gegensatz zu seinem Kommentar von Ziffer 4.6 anstelle der Streichung eine Vereinfachung vor. Neben den Kantonen *NW* und *ZH* fordern auch die *K3* und der *VZK* die Streichung von Ziffer 4.7. Sie schreiben, dass die Regelung im Grundsatz richtig sei, jedoch zu detailliert ausfalle. Die *ISSS* fordert zusätzliche Ziffern mit folgendem Wortlaut: „4.7.4 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens vierteljährlich automatisierte Schwachstellen-Scans durchführen“ und „4.7.5 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens jährlich einen Penetration-Test durch einen unabhängigen Anbieter durchführen lassen“. Der *VAKA* begrüsst grundsätzlich den Vorschlag gemäss Ziffer 4.7, sieht es aber als relativ grossen Aufwand an, sämtliche Software jederzeit auf alle Schwachstellen geprüft zu haben. Zudem handle es sich häufig um closed source Software, sodass eine Sicherheitslücke im Regelfall sowieso unbekannt sei.

4.8 Verwaltung schützenswerter Daten und Systeme (Art. 1 Bst. c und d)

Die *K3*, der *VZK*, der *ZAD* sowie die Kantone *NW* und *ZH* erachten die Regelung als zu detailliert. Der Praxisnutzen schätzen sie als klein ein und wünschen eine Vereinfachung von Ziffer 4.8.

4.8.1: 6 Kantone[116] weisen darauf hin, dass dies Teil der Sorgfaltspflicht sei, welche die Gesundheitsfachpersonen, wie bereits in der heutigen Praxis, einhalten müssten. *Bleuer* macht geltend, dass die Behandlungsrelevanz nicht a priori definiert werden könne. Der *VAKA* schreibt, dass die Entscheidung gemäss Ziffer 4.8.1 durch die Gesundheitsfachpersonen getroffen werde und im Einzelfall zu beurteilen sei. Das *KSSG* fragt, wie diese Vorgaben erfüllt werden sollen, wenn es keine Richtlinie gebe, welche Daten behandlungsrelevant sind. Ähnlich fragen die *BINT* und die *Integic*, wie „behandlungsrelevant“ in diesem Zusammenhang zu verstehen sei und geben zu bedenken, dass das Verständnis dazu einem erheblichen Wandel unterworfen sein dürfte. Die *SGMI* bezeichnet die Definition „behandlungsrelevant“ ebenfalls als zu wenig genau und wünscht, wie dies bereits in der Stellungnahme zum Gesetzesentwurf von 2011 der Fall gewesen sei, eine Konkretisierung. Des Weiteren kritisiert auch der *VGIch*, dass es unklar sei, welche Daten / Dokumente als behandlungsrelevant gelten. Während insgesamt 9 Stellungnehmende[117] die alternativlose Streichung von Ziffer 4.8.1 fordern, wäre für die *Integic* und den *KSSG* auch eine Präzisierung denkbar. Der *VGIch* schlägt seinerseits vor, dass das BAG ein unverbindliches Template für einen Best Practice der Dokumentenbereitstellung durch die Spitäler liefern solle. Die *OFAC* fragt, wie die Gemeinschaft irgendetwas betreffend den angeschlossenen Gesundheitseinrichtungen gewährleisten könne. Wer würde wie und nach welchem Recht die Kontrolle über die Zeit sicherstellen? Die Aufgaben der Gemeinschaften seien umfassend in Artikel 10 EPDG beschrieben. Die angeschlossenen Gesundheitseinrichtungen seien, unabhängig von ihrer Mitgliedschaft, dem Schweizerischen Datenschutzrecht unterworfen. Dazu müsse noch erwähnt werden, dass es auch von der Rechtsform abhänge, welchem Recht die Einrichtungen unterworfen sind.

4.8.2 – 4.8.4: Die *Post* wiederholt ihre Stellungnahme von Ziffer 4.5 in Bezug auf Ziffer 4.8.2. 6 Kantone[118] machen darauf aufmerksam, dass der in der französischen Version verwendete Begriff „sensible“ bei Ziffer 4.8.2 nicht den gleichen Sinn habe wie in den Artikeln 1 und 2 EPDV oder in dem EPDG, was eine Klärung nötig mache. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* weisen darauf hin,

[116] FR, NE, GE, VS, VD, JU
[117] VAKA, BINT, FR, NE, GE, VS, VD, JU, Bleuer
[118] FR, NE, GE, VS, VD, JU

dass wiederum der Begriff „schützenswerte Daten“ verwendet wird, ohne dass diese Bezeichnung eine Definition erfahren hätte. Dies führe zu Rechtsunsicherheiten. Sie regen an, eine Legaldefinition aufzunehmen. Für die *Integic* impliziere Ziffer 4.8.3.8.1, dass je IHE-Actor ein eigenes Client Zertifikat zu verwenden sei und bittet um eine Klarstellung. Das *KSSG* schreibt zu dieser Ziffer, dass die Speicherung des TLS-Clientzertifikates im Inventar unsicher sei. Die Clientzertifikate würden an einen geschützten Ort gehören. Es wird die Löschung der Ziffer oder eine Umformulierung gewünscht. Das Inventar solle nur den Namen des Clientzertifikates enthalten, jedoch nicht das Zertifikat selbst. 6 Kantone[119] weisen darauf hin, dass eine Gemeinschaft nicht ein Inventar mit tausenden von Primärsystemen halten könne und auch nicht Informationen über das TLS-Zertifikat, welches auf den Systemen installiert ist, zur Verfügung stellen könne. Sie fordern die Streichung von Ziffer 4.8.3.8. Die *SQS* bemängelt, dass der Satz von Ziffer 4.8.4.3 nicht verständlich sei. Es sei unklar, um was für eine Bestätigung es sich handle, weswegen eine Präzisierung resp. Neuformulierung vorzunehmen sei. Die *ahdis* wünscht, dass Ziffer 4.8.3.8.1 auf „die Serial ID, HASH des TLS-Clientzertifikats“, anstelle von „TLS-Clientzertifikat“ präzisiert wird, damit das Missbrauchspotenzial limitiert werde. Die *OFAC* schreibt betreffend dem Primärsystem als IHE-Akteur, dass es in der Liste an Schnittstellen zwischen der Gemeinschaft und dem Rest der Welt fehle. Es bestehe keine Anforderung, dass der Transport und der Austausch zwischen dem Primärsystem und der Gemeinschaft nach dem IHE-Protokoll erfolgen müsse. Allgemein müssten alle Verbindungen zwischen der Gemeinschaft und Dritten Teil des Inventars als Schnittstelle sein.

4.9 Datenschutz- und Datensicherheitsanforderungen für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen, sowie Endgeräte (Bst. e)

HIN begrüsst, dass die Anforderungen an das Endgerät aufgeführt sind. Die *SGMI* und die *FMH* kritisieren, dass die Anforderungen an angeschlossene Gesundheitseinrichtungen und deren Gesundheitsfachpersonen in die Hoheit der Primärsysteme eingreifen würden. Sie fordern die Überarbeitung des gesamten Abschnittes, insbesondere Streichung der Ziffern 4.9.1.2.3, 4.9.2 und 4.9.3. Gemäss dem *VGIch* darf sich das SIEM nur auf die technischen und organisatorischen Teile der Gemeinschaftsinfrastruktur beschränken, welche der Bereitstellung des elektronischen Patientendossiers dienen, nicht aber auf (logisch getrennte) Erweiterungen zur Bereitstellung gerichteter Kommunikation und nicht auf die Infrastruktur und Organisation der angeschlossenen Institutionen angewendet werden. Es sei mit einer eigenen Ziffer explizit abzugrenzen. Die *OFAC* kritisiert, dass die Gemeinschaften nichts betreffend angeschlossenen Einrichtungen garantieren können, von denen sie weder die Eigentümer noch die Verantwortlichen seien. Die Rolle der Gemeinschaften gegenüber den angeschlossenen Einrichtungen sei auf die Beschreibung der technischen und organisatorischen Anforderungen ihrer Schnittstellen limitiert.

4.9.2 / 4.9.3: Sichere Endgeräte für Gesundheitsfachpersonen: Die *BINT* schreibt, dass mit Ziffer 4.9.2 die Verantwortung auf die Angeschlossenen verlagert werde, was in diesem Sinne in Ordnung sei. Es könne jedoch nicht durchgesetzt bzw. sanktioniert werden und zudem greife es über die Zuständigkeitsgrenze des EPDG hinaus, weswegen die Ziffer zu streichen sei. Die *ISSS* würde einen Text inkl. Beispielkatalog bevorzugen und schlägt deshalb folgende Formulierung vor: „[…] Endgeräte sicherzustellen (z.B. auch speziell eingeschränkt für Internet-Nutzung, Visual- oder Audio-Aufnahmen, Datentransfers, Synchronisationen), die von den Gesundheitsfachpersonen […]“. Die *Post* gibt betreffend den Ziffern 4.9.2 und 4.9.3 zu bedenken, dass die Gemeinschaften nicht einzelne angeschlossene Computer kontrollieren und validieren können. Diese Anforderung an die Gemeinschaften sei nicht umsetzbar und die Gemeinschaften sollen in den AGB für die Benutzer die Sicherheitsanforderungen definieren. Die *Integic* schreibt in ihrem Kommentar zu Ziffer 4.9.3 folgendes: „Personenspezifische Benutzer und definitives Verbot / Verweigerung von Sammel- oder Gruppenbenutzerzugängen“ und wünscht eine Ergänzung der Ziffer. Gemäss dem *VGIch* stelle Ziffer 4.9.3 einen Eingriff in die Betriebskompetenz der Spitäler dar, weshalb die Bestimmung wegzulassen sei. Eine diesbezügliche Vereinbarung zwischen Gemeinschaft und Institution genüge völlig. Für die *K3*, den *VZK*, den *ZAD* und den Kanton *ZH* handle es sich um Selbstverständlichkeiten, die in der Praxis ohnehin beachtet werden dürften. Ziffer 4.9.3 sei

[119] FR, NE, GE, VS, VD, JU

zu streichen, oder, falls daran festgehalten wird, zu vereinfachen mittels einer generell-abstrakten Regelung in der EPDV. Der *VAKA*, die *K3* und der *VZK* machen darauf aufmerksam, dass eine Firewall kein Element auf dem Endgerät der Gesundheitsfachperson sei und schlagen die Streichung des relevanten Textes oder die Anpassung des Absatztitels vor. Die *OFAC* schreibt, dass die Beziehung zwischen der Gemeinschaft und den angeschlossenen Gesundheitseinrichtungen rein vertraglicher Natur sei. Falls das BAG entscheide, die Gesundheitsfachpersonen Regelungen und strengen Normen in Bezug auf der Informationssicherheit und Datenschutz zu unterwerfen, sollte das nicht durch das elektronische Patientendossier passieren. Es bestehe keine gesetzliche Grundlage dafür im EPDG.

4.10 Datenschutz- und Datensicherheitsanforderungen an das Personal (Abs. 1 Bst. f)

Der *ZAD* sowie die Kantone *NW* und *ZH* wiederholen ihre Stellungnahme von Ziffer 4.6, welcher sich betreffend Ziffer 4.10 auch die *K3* und der *VZK* anschliessen.

4.10.1: Die *ÄTG* und der *HÄ CH* weisen darauf hin, dass der Datenschutz und ein korrekter Umgang mit sensiblen Daten für Gesundheitsfachpersonen bereits heute wichtige Aufgaben seien. Bei der Umsetzung der geforderten Ziele durch die Gemeinschaften sei allerdings darauf zu achten, dass die Vorgaben mit Vernunft, Augenmass und verhältnismässigem zeitlichen und finanziellen Aufwand zu erreichen seien (Grenznutzen). Die *Post* fragt, ob es hier um den Betrieb der Systeme des EPDG, wie Administration, Engineering, Helpdesk, etc. gehe und wünscht eine Konkretisierung.

4.10.2: 6 Kantone[120] schreiben betreffend Ziffer 4.10.2.1, dass die Gemeinschaft nicht garantieren könne, dass die Personen ihre Verantwortung wahrnehmen oder dass diese kompetent sind. Es sei nicht an der Gemeinschaft, für die Beurteilung der Anwenderkenntnisse Verantwortung zu übernehmen, weshalb die Ziffer zu streichen sei. Die *GDK* und 6 Kantone[121] kritisieren, dass sich die Vorgabe gemäss Ziffer 4.10.2.3 nicht umsetzen lasse. Eine vertragliche Verpflichtung der Personen, die Zugriff auf Daten des elektronischen Patientendossiers haben, in Analogie zur ärztlichen Schweigepflicht, sei nicht justiziabel. Dasselbe geben weitere 7 Stellungnehmende[122] zu bedenken. Sie fügen an, dass die ärztliche Schweigepflicht durch Bundesrecht und allenfalls ergänzendes kantonales Recht geregelt sei. Weder Gemeinschaften noch Stammgemeinschaften würden dazu Regelungskompetenzen besitzen. Gemäss der *K3*, dem *VZK* und dem *ZAD* sollte abgeklärt werden, inwiefern Mitarbeitende von Gemeinschaften und Stammgemeinschaften als Hilfspersonen im Sinne von Artikel 321 Schweizerisches Strafgesetzbuch (StGB) angesehen werden können. Der Kanton *ZH* schreibt diesbezüglich, dass Mitarbeitende von Stammgemeinschaften und Gemeinschaften von Artikel 321 StGB nicht erfasst würden und ohne Anpassung der StGB die Strafbarkeit der Ärztinnen und Ärzte nur entfalle, wenn eine rechtsgenügende Einwilligung der Patientin / des Patienten im Sinne von Artikel 321 Ziffer 2 StGB vorliege. Ähnlich fragt die *SQS*, was unter einer der ärztlichen Schweigepflicht analoge Verpflichtung zu verstehen sei. Die ärztliche Schweigepflicht gehöre zu den Schweigepflichten nach Artikel 321 StGB. Die Aufzählung der betroffenen Berufe sei abschliessend und betreffe zu den Ärztinnen / Ärzten hin ausschliesslich deren Hilfspersonen. Nicht unter die ärztliche Schweigepflicht würden insbesondere IT-Dienstleister fallen. Ziffer 4.10.2.3 sei zu präzisieren resp. folgendermassen umzuformulieren: „[…] erlangen könnten, müssen entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet sein. Die vertragliche Schweigepflicht muss alle Daten des elektronischen Patientendossiers betreffen, welche im Rahmen der Berufsausübung den Personen bekannt werden und sie muss unbefristet über die Berufsausübung und über Ende des Auftrags hinaus gelten“. Die *Tessaris* schreibt zu 4.10.2.3, dass die nicht dem, bei seiner Verletzung mit Strafe bedrohten, ärztlichen Berufsgeheimnis unterstellten und verpflichteten Personen (z.B. Angestellte der Betriebsorganisationen nach Ziffer 4.1.1) durch entsprechende Massnahmen (schriftliche Vertraulichkeitsverpflichtung) zur Einhaltung strenger Vertraulichkeit verpflichtet werden sollten. Deshalb wird folgender Text für die Ziffer vorgeschlagen: „Personen, die Zugang zu Daten des elektronischen Patientendossiers erhalten, müssen durch geeignete Massnahmen, insbesondere Unterzeichnung einer Vertraulichkeitsverpflichtung,

[120] FR, NE, GE, VS, VD, JU
[121] BL, GL, LU, OW, UR, SZ
[122] NW, ZG, ZH, TI, ZAD, K3, VZK

zur Geheimhaltung der bei Ausübung ihrer Tätigkeit für die Gemeinschaft wahrgenommenen Informationen über Patientinnen oder Patienten angehalten werden". Die *ISSS* macht folgenden Präzisierungsvorschlag für Ziffer 4.10.2.3: „[…] analogen Verpflichtungen (wie z.B. einer vertraglichen Geheimhaltungspflicht) unterliegen". Für den Kanton *AR* stellen sich bezüglich Ziffer 4.10.2.3 die Fragen resp. sei zu präzisieren, welche Personen damit abgedeckt werden, wer „kompetent" ist und was in diesem Zusammenhang „bewusst" heisse. Insgesamt sprechen sich 14 Stellungnehmende[123] für die Streichung von Ziffer 4.10.2.3 aus. Die *Tessaris* schreibt bezüglich Ziffer 4.10.2.4, dass die Anforderungen an das Personalmanagement auf die Aspekte von Datenschutz und Datensicherheit ausgerichtet sein sollten und schlägt dementsprechend folgende Formulierung vor: „auf die Anforderungen an Datenschutz und Datensicherheit ausgerichtete Prozesse […]".

4.10.3: Die *SGMI* erachtet die Ziffer 4.10.3 sowie die Unterziffern als unverhältnismässig und fordert deren Streichung. Der Kanton *ZH* wiederholt seine Stellungnahme von den Ziffern 4.6 und 4.10. Die *Post* bittet im Rahmen der Ziffer 4.10.3 um exaktes referenzieren auf andere Gesetze, damit die konkrete Vorschrift nachgelesen werden könne. Für die *IG eHealth* stellt sich die Frage, ob der Grundsatz der Rechtsgleichheit nicht verletzt werde, 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 liege. Sie empfiehlt diesen Punkt mit den kantonalen Anforderungen zu harmonisieren. Gemäss dem Kanton *BS* seien die Ziffern 4.10.3.1 und 4.10.3.2 dahingehend zu präzisieren, dass sich die „Liste der Schlüsselpersonen" nicht auf Gesundheitsfachpersonen beziehe. Es müsse klar sein, dass die Gesundheitsfachpersonen keine Personensicherheitsprüfung nach Militärgesetz durchlaufen müssen. Die Personensicherheitsprüfung nach Militärgesetz müsse für die Stammgemeinschaften ohne grossen Aufwand abgewickelt werden können. Folgender Zusatz für Ziffer 4.10.3.1 wird vorgeschlagen: „[…] Liste aller Personen, welche keine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG sind, führen, die […]". Die *privatim* schreiben, dass die Regelung gemäss Ziffer 4.10.3.1 aus datenschutzrechtlicher Sicht zwar zu begrüssen sei, jedoch unklar erscheine, welche Personen diese Liste tatsächlich umfassen solle. Es könnten kaum alle Gesundheitsfachpersonen, die auf das elektronische Patientendossier zugreifen können Schlüsselpersonen sein. Die Regelung sei zu präzisieren. 6 Kantone[124] wünschen die Klärung von Ziffer 4.10.3.1 mittels der Angabe konkreter Beispiele.

Gemäss 15 Stellungnehmenden[125] sei nicht ersichtlich, wie eine Gemeinschaft oder Stammgemeinschaft eine „PSP nach Militärgesetz" durchführen können solle. 6 Stellungnehmende[126] fügen hinzu, dass es auch inhaltlich als nicht sachgerecht erscheine, eine solche Überprüfung zu verlangen. Die *Insel*, die *Integic* und der *KSSG* bemängeln, dass diese Forderung im Quervergleich mit anderen Institutionen unverhältnismässig sei, während die *STSAG* die Bezeichnung „inadäquater Aufwand" für die Vorgabe gemäss Ziffer 4.10.2.3 wählt. *Bleuer* schreibt dazu, dass die Forderung ein unverhältnismässiger Eingriff in die Persönlichkeitsrechte der betroffenen Arbeitnehmer sei und dass die gesetzliche Grundlage bzw. Rechtmässigkeit fraglich sei, was auch die *Integic* bemängelt. Die *SQS* schreibt, dass für PSP eine gesetzliche Grundlage notwendig sei, die Ergebnisse dürften nur an die in Spezialgesetzen bestimmten spezifischen Adressaten bekanntgegeben werden. Es fehle eine genügende gesetzliche Grundlage für diese Regelung bzw. aufgrund des Legalitätsprinzips reiche es nicht aus, dass in einem Anhang einer departementalen Verordnung dieser Nachweis verlangt werde. Die *SUVA* weist darauf hin, dass die PSP weder im Militärgesetz selbst noch in der Verordnung über die PSP (PSPV) vorgesehen sei. Es stelle sich die Frage der gesetzlichen Legitimation einer solchen strengen Prüfung und des Weiteren sei auch die Verhältnismässigkeit nicht mehr gewährleistet. Eine solche Bestimmung sei mit dem heutigen Recht nicht vereinbar und angesichts der heutigen datenschutzrechtlichen Möglichkeiten nicht nötig. *SCH* macht ebenfalls die mangelnde Verhältnismässigkeit geltend und ist der Meinung, dass es den Interessensgemeinschaften obliege, Empfehlungen zur Integritätsprüfung von Personen, die Zugriff auf Patientendaten haben, zu machen. Die *Tessaris* schreibt, dass sich nach der hier vertretenen

[123] K3, VZK, ZAD, GDK, BL, GL, LU, OW, UR, SZ, NW, ZG, ZH, TI
[124] FR, NE, GE, VS, VD, JU
[125] GDK, BL, GL, LU, OW, UR, AR, SZ, NW, TG, ZG, ZH, ZAD, K3, VZK
[126] K3, VZK, ZAD, ZH, NW, ZG

Auffassung die im Militärgesetz und im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vorgesehene PSP auf die Schlüsselpersonen nach dem EPDG nicht anwenden lasse. PSP nach diesen Gesetzen setzen Einsicht in das Strafregister und die Beschaffung von Daten über die Privatsphäre der geprüften Person voraus, d.h. einen Eingriff in Grundrechte, der durch ein formelles Gesetz gerechtfertigt werden müsse. Das *KSSG* gibt zu bedenken, dass eine Umsetzung dieser Anforderungen innerhalb der gegebenen Frist von 3 Jahren unrealistisch sei. Die *BINT* kritisiert, dass die PSP den Einsatz von ausländischen Arbeitskräften verhindere. Der *VGIch* schreibt, dass Ziffer 4.10.3.2 unverhältnismässig sei und die Gleichbehandlung mit Gesundheitsfachpersonen verletze. Diese Voraussetzung verstosse zudem formal als auch materiell gegen geltende Rechtsgrundsätze.

Insgesamt 26 Stellungnehmende[127] fordern die Streichung von Ziffer 4.10.3.2. 6 Kantone[128] geben zu bedenken, dass die PSPV nicht an diesen Zusammenhang angepasst sei. *SCH* würde alternativ zur Streichung auch folgenden Text befürworten: „diese Personen eine adäquate Integritätsprüfung durchlaufen haben" und für die *Tessaris* käme auch in Frage festzustellen, ob diese Personen eine PSP nach der Gesetzgebung des Bundes oder des zuständigen Kantons durchlaufen haben und gegebenenfalls um die Durchführung einer PSP ersuchen. Der *VAKA* wünscht generell eine Anpassung der Formulierung von Ziffer 4.10.3.2. Der Kanton *BS* schlägt folgende Zusatz für die Ziffer vor: „[…] PSP in Anlehnung an das Militärgesetz […]". *HIN* weist darauf hin, dass bei Ziffer 4.10.3.2 ein Verb fehle (vermutlich „dafür sorgen, dass"), womit der Text zu ergänzen sei. Die *ISSS* fragt, ob die PSP nur initial durchlaufen werden müsse, oder ob diese regelmässig zu wiederholen sei und macht folgenden Formulierungsvorschlag: „diese Personen vor Aufnahme ihrer Tätigkeit und in begründeten Fällen auch während ihrer Tätigkeit eine PSP nach […]". Die *Tessaris* schreibt bezüglich Ziffer 4.10.3.3, dass die Gemeinschaften nicht die Kompetenz hätten, um „offiziell festgelegte" Verfahren vorzusehen, weshalb diese Bezeichnung anfangs der Ziffer zu streichen sei.

4.11 Datenschutz- und Datensicherheitsanforderungen an Dritte (Abs. 1 Bst. f)

Gemäss der *K3*, dem *VZK*, dem *ZAD* sowie den Kantonen *ZH* und *NW* sei zu prüfen, ob die Bestimmungen unter Ziffer 4.11 erforderlich sind. Falls ja sei zu prüfen, ob diese nicht durch einfachere, generell-abstrakte Regelungen in der EPDV ersetzt werden können. Die *OFAC* fragt, weshalb sich unter Ziffer 4.11 keine Referenz auf die Anforderungen von Artikel 10 Absatz a DSG finden lasse. Die *Post* schreibt bezüglich Ziffer 4.11.1, dass das Verzeichnis von Dritten Sinn mache. Sie fragt zudem, was das Visum des Datensicherheitsverantwortlichen bezwecke. Die Formulierung scheine etwas sehr offen. Der Begriff „IT-Infrastrukturkomponenten" sollte etwas enger gefasst werden, da sonst auch Intel, Samsung, Microsoft etc. auf diese Liste müssten. Sie beantragt, dass die Forderung nach Visum und die Formulierung „unter Umständen" gelöscht werden. Die *SQS* macht bezüglich Ziffer 4.11.2 darauf aufmerksam, dass der erste Satz sprachlich wie folgt vervollständigt werden müsse: „Gemeinschaften müssen sicherstellen, dass kein Datenzugriff […]". Die *Tessaris* kritisiert, dass Ziffer 4.11.2 schon orthographisch nicht ganz korrekt formuliert sei. Darüber hinaus sei nicht ganz klar, was an dieser Stelle mit „Intermediäre" im Unterschied zu „Dritte" gemeint ist. Die *Post* fragt, worin der Unterschied zwischen Ziffer 4.11.3 und Ziffer 4.11.4 bestehe. Gemäss der *privatim* sollten die Verträge gemäss Ziffer 4.11.5 zwingend ebenfalls folgende Klauseln enthalten: Regel wonach der Dritte sicherzustellen hat, dass nur jene seiner Mitarbeitenden Zugriff auf die Daten haben, die diese zur Aufgabenerfüllung tatsächlich benötigen; Die Mitarbeitenden mittels Verschwiegenheitserklärung, die über die Beendigung des Arbeitsverhältnisses hinaus Gültigkeit hat, zur Verschwiegenheit zu verpflichten; Keine Weitergabe von Daten an Dritte ohne Einverständnis der Gemeinschaft. Zudem solle die Regelung in Ziffer 4.11.5.4 präzisiert werden bezüglich wer das Recht zur regelmässigen Überprüfung habe. Die Betreiber der Gemeinschaft, oder der Datenschutzbeauftragte der Gemeinschaft? Ebenfalls solle geregelt werden, dass die Gemeinschaft befugt ist, zu dieser Überprüfung qualifizierte Dritte beizuziehen. Des Weiteren fordern die *privatim* auch eine Umformulierung der Ziffern 4.11.5.5 bis 4.11.5.7. Untervertragsverhältnisse sollen möglichst vermieden werden. Je mehr Beteiligte vorhanden sind, desto schwieriger würden sich

[127] BINT, Bleuer, Insel, Integic, KSSG, GDK, BL, GL, LU, OW, UR, AR, SZ, NW, TG, ZG, ZH, ZAD, K3, VZK, SQS, STSAG, SUVA, SCH, Tessaris, VGIch

[128] FR, NE, GE, VS, VD, JU

die Übersicht und die Kontrolle gestalten. Die Regelung solle dahingehend umformuliert werden, dass Untervertragsverhältnisse nur im Ausnahmefall und nur mit dem Einverständnis der Gemeinschaft (im konkreten Fall – keine Generalzustimmung) zulässig seien.

4.12 Überwachung und Überprüfung von Dienstleistungen (Abs. 1 Bst. f)

Die *K3*, der *VZK*, der *ZAD* und der Kanton *ZH* wiederholen ihre Stellungnahme von Ziffer 4.11. Die *SQS* wiederholt ihre Bemerkung von Artikel 11 Absatz 2 EPDV und bezüglich Ziffer 4.12.1 und schlägt vor, die Zertifizierungsstelle als Meldestelle für als sicherheitsrelevant eingestufte Vorfälle zu streichen.

4.13 Meldepflicht für Sicherheitsvorfälle (Abs. 2)

Die *K3*, der *VZK*, der *ZAD* und der Kanton *ZH* wiederholen ihre Stellungnahme von Ziffer 4.11 sowie 4.12 und die *FMH* wiederholt ihren Kommentar von Ziffer 4.5.1.1. Die *SQS* plädiert dafür, dass Zertifizierungsstellen nicht als Meldestelle für Sicherheitsvorfälle vorzusehen seien. Insofern sei an dieser Stelle auch kein Meldeverfahren durch die Gemeinschaften zu definieren. Sie schlägt vor, die Zertifizierungsstelle als Meldestelle resp. den Textteil „die Zertifizierungsstelle und" aus Ziffer 4.13.1 zu streichen. Die *ISSS* weist darauf hin, dass entsprechend den Vorgaben in anderen Zusammenhängen, z.B. der EU DSGVO, die Information über sicherheitsrelevante Vorgänge auch gegenüber den betroffenen Patientinnen / Patienten zu erfolgen habe, wenn für diese voraussichtlich ein hohe Risiko bestehe. Die Ziffer 4.13.1 sei um den folgenden Satz zu ergänzen: „[…] Zudem müssen Gemeinschaften formale Verfahren für das unverzügliche Melden von Vorfällen an die betroffenen Patienten, durch welche die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Patienten zur Folge hat, definiert haben".

4.14 Betriebssicherheit (Abs. 3)

4.14.1: *HIN* bemerkt zu Ziffer 4.14.1.1.1, dass es sich um eine starke 2-Faktor-Authentisierung handle, was zu begrüssen sei. Die *SQS* stellt zur selben Ziffer die Frage, ab wann eine 2-Faktor-Authentifizierung als stark bezeichnet werden könne und bittet um eine Präzisierung. Das *KSSG* schreibt bezüglich Ziffer 4.14.1.1, dass die Umsetzung einer 2-Faktor-Authentifizierung bei den Betriebssystemen, vor allem aber den Datenbanken und anderen technischen Komponenten als unverhältnismässig und nur schwierig umsetzbar angesehen werden. Das würde bedeuten, dass für alle Benutzer im Active Directory für jeden Zweck (auch ausserhalb des elektronischen Patientendossiers) eine 2-Faktor-Authentifizierung eingesetzt werden müsste was extrem teuer und vor allem nicht mehr praktikabel im Betrieb wäre. Eine 2-Faktor-Authentifizierung auf Datenbanken sei je nach Datenbank gar nicht umsetzbar. Die Ziffer 4.14.1.1 sei dementsprechend zu streichen. Die *STSAG* befürchtet, dass im Zuge der Ziffern 4.14.1.1 sowie 4.14.1.3 – 4.14.1.10 ein inadäquater Aufwand entstehe und spricht sich für die ersatzlose Streichung dieser Bestimmungen aus. 10 Stellungnehmende[129] machen darauf aufmerksam, dass bei Ziffer 4.14.1.1.2 der Satz unvollständig ist und mindestens ein Wort fehle. Der Text sei folglich zu vervollständigen. *HIN* schlägt konkret vor, das Wort „System" an dieser Stelle einzufügen. Gemäss 6 Kantonen[130] erscheine es schwierig sicherzustellen, dass das System keinen Export von Patientendaten ermöglicht, wenn der privilegierte Zugriff den Zugriff auf Patientendaten zulässt. Dieser privilegierte Zugriff beruht auf dem Berufsgeheimnis. Die erwähnten Kantone fordern die Streichung der Ziffer 4.14.1.1.3. Die *ISSS* bezeichnet Ziffer 4.14.1.2.3 als praxisfern. Wenn der Lieferant die Infrastruktur und somit auch deren fortlaufenden Betrieb sicherstellen müsse, dann könnten Zugriffe nicht erst "bei Bedarf" aktiviert werden. SLAs könnten so nicht eingehalten werden (vgl. 4.23.1.2). Die Ziffer sei zu streichen. Weiter macht die *ISSS* folgenden Präzisierungsvorschlag für 4.14.1.4: „[…] diese verschlüsselt, örtlich getrennt und sicher aufbewahrt sind". Bezüglich Ziffer 4.14.1.5 kritisiert sie, dass unklar sei, was mit dieser Regelung bzw. dem 4-Augen-Prinzip gemeint ist. Vermutlich dürfe das Passwort nicht nur einer Person bekannt sein. Aber wie dies technisch aussehen soll, müsse unbedingt erläutert und an-

[129] KKA, BüAeV, GAeSO, KAeG SG, HIN, Post, privatim, medshare, Medgate, SQS
[130] FR, NE, GE, VS, VD, JU

sonsten gestrichen werden. Das *KSSG* schreibt zu den Ziffern 4.14.1.4 und 4.14.1.5, dass die Verschlüsselung der Backups und der Zugang zum Schlüsselmaterial im 4-Augen-Prinzip nicht verhältnismässig seien. Für das elektronische Patientendossier müsse eine separate Backupinfrastruktur aufgebaut werden, was enorme Kosten verursache. Die Ziffern sollen daher so umformuliert werden, dass Backups sicher aufbewahrt werden müssen. Wie das konkret gelöst wird, sei den IT-Betreibern zu überlassen. *HIN* macht darauf aufmerksam, dass das in Ziffer 4.14.1.7 Geforderte automatisiert geschehe, sofern ein Lieferant den Betrieb der IT-Infrastruktur übernimmt und dort regelmässig entsprechende Backups erstellt werden. Eine Trennung des Speichers sei somit unrealistisch, da dies manuelle Tätigkeiten bedeuten würde. Die Ziffer könne somit gestrichen werden. Der *VAKA* wünscht ebenfalls die Streichung dieser Ziffer, da hier die Anforderung (Trennung des Netzwerks bei Backup) wohl überschossen werde. Ähnlich bezeichnet die *Post* die Trennung des Netzwerks als übertrieben. Die Backups seien schon verschlüsselt und die Schlüssel nach dem 4-Augen-Prinzip geschützt. *SCH* schreibt dazu, dass für Cloud Architekturen Backup-Speichersysteme, welche nach dem Kopieren vom Netzwerk getrennt werden müssen, i.A. nicht mehr vorgesehen seien, weil die Aufbewahrung mit den in der ISO 27001 vorgeschriebenen Sicherheitskriterien (Verschlüsselung, 4-Augen-Prinzip bei Zugriff, etc.) als sicher betrachtet werden. *SCH* beantragt ebenfalls die Streichung der Ziffer. *HIN* ist der Meinung, dass bezüglich der Ziffer 4.14.1.11 eine Präzisierung bezüglich der Löschmethode erforderlich sei, analog Ziffer 2.1, und schlägt entsprechend folgenden Zusatz vor: „[…] vorgängig alle Daten kontrolliert und dokumentiert, vollständig und unwiderruflich gemäss aktuellen Best Practice Regeln gelöscht werden". Gemäss der *privatim* sei Ziffer 4.14.1.11 zudem aus datenschutzrechtlicher Sicht zu unpräzise formuliert und schlägt daher den folgenden Text vor: „Patientendaten auf Datenträgern, die nicht mehr benötigt werden, unwiderruflich gelöscht und die Datenträger anschliessend korrekt entsorgt werden". Die *SQS* weist darauf hin, dass die Bestimmung gemäss Ziffer 4.14.1.12 bereits unter Ziffer 2.9.25 geregelt sei, weswegen sie gelöscht werden sollte.

4.14.2 / 4.14.3: Die *ISSS* fragt bezüglich Ziffer 4.14.2.5, ob es wirklich für alle Systeme dedizierte Komponenten in einer separaten Netzwerkzone brauche und schlägt folgende Änderung der Formulierung vor: „[…] mittels geeigneter Trennung isoliert sein (bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich)". Die *STSAG* kritisiert, dass aufgrund der Forderungen unter Ziffer 4.14.2 ein inadäquater Aufwand entstehe, weswegen die darunter aufgeführten Ziffern zu streichen seien. 6 Kantone[131] schreiben betreffend der Ziffer 4.14.3, dass die zu erfüllenden Anforderungen eine hohe Belastung darstellen und wesentliche Kosten verursachen werden. Dies erlaube, dass für die vollständige Zertifizierung eine Zeitspanne von 5 Jahren erlaubt wird. Das *KSSG* fragt, wie die Bestimmung gemäss Ziffer 4.13.3.4 zu erfolgen habe, ob ein Change Management dafür ausreiche oder ein Automatismus (Applikation) dafür eingesetzt werden müsse. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* wiederholen für Ziffer 4.14.3.10 ihre Stellungnahme von Ziffer 4.8.2. *SCH* gibt betreffend der Ziffer 4.14.3.10 zu bedenken, dass das Ausdrucken von Daten und Dokumenten als manuelle Aktion im Systembetrieb nicht an das integrierte Protokollsystem angeschlossen sei. Das Drucken könne damit nicht oder nur mit sehr hohem Aufwand automatisiert und revisionssicher umgesetzt werden.

4.15 Anschaffung, Entwicklung und Instandhaltung von Systemen (Abs. 3)

Das *KSSG* erachtet eine Beaufsichtigung der Entwicklungsfirmen durch die Gemeinschaft als nicht realisierbar und fordert die Streichung der kompletten Ziffer 4.15. Ebenfalls die Streichung wünschen die *K3*, der *VZK*, der *ZAD* und der Kanton *ZH*, für welche die Bestimmungen als entbehrlich erscheinen. Die *Integic* weist darauf hin, dass die Punkte gemäss Ziffer 4.15.2 im Kontext von Konstellationen mit externen Herstellern schwer realisierbar seien und entsprechende Einbindung der Hersteller erfordern würden. Realistisch sei dies kaum möglich, was eine Überarbeitung nötig mache. Gemäss der *GDK* und 8 Kantonen[132] sei es nicht möglich, Testumgebungen ohne Patientendaten zu betreiben, wenn damit Integrations- und Konsolidierungsumgebungen gemeint seien. Es sei mit technischen und organisatori-

[131] FR, NE, GE, VS, VD, JU
[132] BL, GL, LU, OW, UR, FR, BS, SZ

schen Mitteln sicherzustellen, dass Patientendaten in einer Testumgebung des elektronischen Patientendossiers in gleicher Weise geschützt sind wie die Daten in der Produktivumgebung, für was auch das *KSSG* plädiert. Es wird folgende Formulierung von Ziffer 4.15.2.5 gefordert: „die Datenschutz- und Datensicherheitsanforderungen, welche die Datenhaltung betreffen, auch für Patientendaten in Konsolidierungs- und Integrationsumgebungen gelten. In anderen Test- und Entwicklungsumgebungen dürfen sich keine Patientendaten befinden". Das *KSSG* fügt in ihrer Bemerkung an, dass an einer Integrationsumgebung auch die Integrationsumgebungen der Primärsysteme angeschlossen seien. In diesen Integrationsumgebungen möchte man explizit mit Echt-Daten testen. Die Ziffer für die Integrationsumgebungen solle gestrichen werden. Der Kanton *AR* macht bezüglich Ziffer 4.15.2.5 darauf aufmerksam, dass im Falle der Verwendung echter Patientendaten in Testumgebungen, diese den Richtlinien des Datenschutzes entsprechen müssen. Die *H+* schreiben, dass für Softwaretests der Gebrauch der Patientendaten im Rahmen der übrigen Gesetzgebung zum elektronischen Patientendossier möglich sein müsse. Ähnlich gibt der *VGIch* an, dass die Nutzung von Patientendaten für Integrations- und Konsolidierungsumgebungen erlaubt sein müsse, solange die DSDS-Vorgaben der Produktivsysteme auch angewendet werden. Für *SQS* wäre die folgende Formulierung von Ziffer 4.15.2.5 realistischer und somit zu bevorzugen: „In Testumgebungen dürfen sich keine echten bzw. nur anonymisierte oder pseudonymisierte Patientendaten befinden". Der *VAKA* und die *Post* fordern die Streichung von Ziffer 4.15.2.6. Der *VAKA* bemängelt, dass unklar sei, was genau bei wem beaufsichtigt werde. Die *Post* fragt ihrerseits, wie das in Bezug auf eingekaufte Software funktioniere und was die Betriebsorganisation mit der Softwareentwicklung zu tun habe. Diese Forderung könne bei der Zertifizierung Probleme bereiten. Die *OFAC* weist darauf hin, dass zwischen Ziffer 4.15.1 und 4.15.5 ein Widerspruch bestehe. Die finale Validierung einer neuen Version brauche vor ihrer Publikation einen Nicht-Regressionstest, der nur mit echten Daten realisierbar sei. Massnahmen könnten umgesetzt werden, so dass die Validierungstests keine Verletzbarkeit verursachen. Sie seien genau so streng zu kontrollieren wie die Produktionssysteme. Es sei mehr eine Verantwortung des Change Managements als eine gesetzliche Vorschrift. Das Prinzip sei, dass man immer einen guten Ausgleich zwischen der Qualität der durchgeführten Tests und dem Respekt der Privatsphäre der Patientinnen / Patienten nachweisen könne.

4.16 Verschlüsselung in der Kommunikation (Abs. 3)

Die *SGMI* und die *FMH* sprechen sich dafür aus, dass sämtliche Kommunikation und Speicherung der Daten verschlüsselt erfolgen solle. Die *STSAG* bezeichnet die Ziffer 4.16.1 innerhalb der Gemeinschaft als übertrieben und fordert die Streichung dieses Textteiles.

4.17 Verschlüsselte Datenspeicherung (Abs. 3)

Die *Insel* fragt bezüglich Ziffer 4.17, ob unter „besonders schützenswerte Daten" alle Patientendaten zu verstehen seien, oder nur sensible und bittet diesbezüglich um eine präzisere Definition. Die *SGMI* sowie die *FMH* wiederholen ihre Stellungnahme von Ziffer 4.16 und die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* wiederholen für Ziffer 4.17.1 ihre Stellungnahme zu den Ziffern 4.8.2 und 4.14.3.10. Des Weiteren wiederholen 6 Kantone[133] ihre Stellungnahme von Ziffer 4.8.2 bezüglich Ziffer 4.17. 13 Stellungnehmende[134] weisen darauf hin, dass entweder alle Daten verschlüsselt werden sollen oder keine. Es leuchte nicht ein, weshalb nur „besonders schützenswerte Daten" zu verschlüsseln sind. Die Vorgabe, dass nur Daten der Klassifizierungsstufen „geheim" und „sensibel" verschlüsselt gespeichert werden müssen, leuchte ebenfalls nicht ein. Einsparungen liessen sich damit nicht erzielen, denn die Kosten für die Verschlüsselungsmöglichkeit würden ohnehin anfallen. Ziffer 4.17.1 sei dementsprechend zu überarbeiten. Den Bedenken, dass keine Kosten eingespart werden können, schliessen sich auch die Kantone *TG* und *AI* an. Sie fordern, dass alle Daten verschlüsselt werden. Der *VAKA* schreibt, dass der Zusatz „und integritätsgeschützt" nicht zielführend erscheine, da die Daten bereits verschlüsselt sind, weshalb dieser zu streichen sei. Zudem macht er darauf aufmerksam, dass die Angaben in den Erläuterungen zur End-zu-End-Verschlüsselung verwundern. Die Argumentation sei nicht nachvollziehbar und die Formulierung „wird vorderhand verzichtet" grenze an eine Drohung. Der *VAKA* sei nicht

[133] FR, NE, GE, VS, VD, JU
[134] GDK, BL, GL, LU, OW, UR, ZG, SZ, ZH, NW, K3, VZK, ZAD

grundsätzlich gegen neue Technologien, trotzdem verwundere, dass eine noch nie in den Gremien von eHealth Suisse diskutierte Technologie, so prominent erwähnt werde. Vor allem, da viele weitere Fragen dazu geklärt werden müssten. Die *Tessaris* macht geltend, dass sich Daten als "besonders schützenswert" im elektronischen Patientendossier qualifizieren dürften, welche sich auf die Gesundheit und die medizinische Behandlung der Patientinnen und Patienten beziehen ("Behandlungsrelevante Informationen"). Daneben gebe es Adress-, Administrations- und Metadaten, die der Verwaltung und dem Betrieb des elektronischen Patientendossiers sowie der Übermittlung der behandlungsrelevanten Daten dienen. Aus praktischen Überlegungen und zur Vermeidung von Abgrenzungsproblemen wäre es möglicherweise vorzuziehen, sowohl die behandlungsrelevanten Patientendaten wie auch die Metadaten verschlüsselt zu speichern. Sie macht folgenden Formulierungsvorschlag: „ Die Daten des elektronischen Patientendossiers, mit Ausnahme der Metadaten, müssen mit geeigneten und dem Stand der Technik entsprechenden kryptographischen […]", oder alternativ: „Die auf die Behandlung der Patientinnen und Patienten bezogenen Daten des elektronischen Patientendossiers müssen […]".

4.19 Kommunikationssicherheit: Verwaltung von Netzwerken (Als. 3)
Die *ISSS* schlägt eine neue Ziffer 4.19.1.4 mit folgender Formulierung vor: „nicht autorisierte WLAN-Zugriffspunkte erkannt und identifiziert werden", gibt aber zu bedenken, dass diese Zusatzanforderung, je nach Interpretation, evtl. bereits durch Ziffer 4.19.1.2 abgedeckt sei.

4.20 Kommunikationssicherheit: Netzwerkdienste (Abs. 3)

4.20.1: 6 Kantone[135] fragen, was die „Informationsdienste, Benutzer und Informationssysteme" seien und wünschen die Angabe konkreter Beispiele für solche Dienste. Der *VAKA* bittet um Prüfung, ob die unter 4.20.1.1 subsumierten Anforderungen nicht schon in ATNA so vorgegeben seien. Falls dem so sei, wäre die Ziffer zu streichen. Die *SQS* wiederholt ihre unter Ziffer 2.9.3 aufgeführte Bemerkung bezüglich den Ziffern 4.20.1.1.2.1 bis 4.20.1.1.5. Sie fordert, dass die Ziffern 2.9.4 bis 2.9.21 mit einer Regelung bezüglich Nachweises technischer Überprüfung der technischen Voraussetzungen ergänzt wird. *SCH* geben bezüglich den Ziffern 4.20.1.1.2.1 und 4.20.1.1.2.2 zu bedenken, dass EV-Zertifikate auch von Sicherheitsexperten kritisiert werden, weil sie nur scheinbar eine höhere Sicherheit als öffentliche TLS-Zertifikate bieten würden, aber höhere Kosten und Verwaltungsaufwände verursachen. Der effektive Schutz eines herkömmlichen Zertifikats und eines EV-Zertifikats könne identisch sein oder beim EV-Zertifikat sogar geringer. Es wird daher die Streichung von „Extended-Validation" aus den beiden Ziffern gefordert. Die *ISSS* spricht sich für die Aufnahme einer neuen Ziffer 4.20.1.1.6 aus mit folgendem Text: „ausschliesslich die für die Systemfunktion notwendigen Dienste, Protokolle und Daemons aktiviert sind".

4.20.2 / 4.20.3: Der *EHS* und der *VGIch* kritisieren, dass Ziffer 4.20.2.1 die Synergienutzung gerichteter und ungerichteter Kommunikation über eine eHealth-Plattform verunmögliche und dadurch unnötige Zusatzkosten verursache bzw. damit den Einsatz proprietärer Systeme für die gerichtete Kommunikation fördere. Eine klare logische Trennung würde genügen. Die Ziffer sei wie folgt anzupassen: „Es werden Massnahmen getroffen, dass die Komponenten (Repository, Registry, Patientenindex) für die sichere Anwendung sowohl gerichteter wie ungerichteter Kommunikation gemäss EPDG/EPDV genutzt werden können", für was sich auch die *Insel* ausspricht. Die *ISSS* bemängelt, dass das in Ziffer 4.20.2.1 aufgeführte Wort „separiert" zu viel Interpretationsspielraum zulasse, weshalb die Ziffer folgendermassen zu ergänzen sei: „[…] aufweisen. Bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich". Der *VAKA* plädiert wiederum für eine Streichung gewisser Textteile, damit Ziffer 4.20.2.1 folgendermassen lautet: „Dokumentenregister, Dokumentenablage, Berechtigungssteuerung und Patientenindex netzwerktechnisch von allen anderen Systemen separieren". Bezüglich Ziffer 4.20.3.1 schreibt *SCH*, dass sogenannte demilitarisierte Zonen (DMZ) nur eine Möglichkeit zur Absicherung von Netzwerken über gestaffelte Zugriffssteuerung mittels Firewalls darstellen und daneben andere Konzepte, die heute insbesondere in Cloud Architekturen genutzt werden, existieren würden. Die *SQS* fragt zu Ziffer 4.20.3.2, gemäss welcher Basis/Vorgabe eine WAF zu betreiben / dokumentieren sei und welche Aspekte der technischen

[135] FR, NE, GE, VS, VD, JU

Implementierung einer WAF zu beachten seien. Eine WAF gebe es als Hardware-Appliance, Software-Plug-In auf einem Webserver oder auch als Addon für Netzwerkfirewalls oder Loadbalancer. Die Dokumentationsanforderung an die HW/SW-Infrastruktur des Zugangsportals sollte generischer formuliert werden. Die Ziffer sei dementsprechend zu ergänzen resp. umzuformulieren.

4.21 Ablauf von Netzwerk-Sitzungen („Session Timeout")

Die *privatim* wünschen aus Gründen der Klarheit eine Umformulierung der Bestimmungen. Zudem sei zu überprüfen, ob 2 Stunden Inaktivitätszeit für Gesundheitsfachpersonen nicht zu lange ist: „Netzwerksitzungen, die während einer definierten Zeitperiode inaktiv sind (nicht bedient werden), sind vom System automatisch zu beenden. Die Inaktivitätsperiode beträgt bei Patienten 20 Minuten und bei Gesundheitsfachpersonen 1 Stunde". Der *VGIch* wiederholt seine Stellungnahme von Ziffer 4.9.3. Die *Insel* schreibt, dass eine so kurze Sessions-Dauer für Patientinnen / Patienten als erhebliche Einschränkung der Benutzbarkeit wahrgenommen werde und schlägt vor, die Bestimmungen an Online-Banking-Lösungen zu orientieren. Die Patientin / der Patient könne selber time-out-Einstellung wählen und ihr / sein Risiko persönlich tragen. Gemäss der *K3*, dem *VZK*, dem *ZAD* und dem Kanton *ZH* erscheine es als wenig sinnvoll, absolute Zahlen für ein automatisches Logout vorzugeben. Eine generell-abstrakte Regelung dürfte genügen. Ziffer 4.21 sei daher zu streichen und durch eine Regelung in der EPDV(-EDI) zu ersetzen. Für die *SQS* ist die Festhaltung der Dauer von Sessiontimeouts wenig sinnvoll. Zudem sei es bedenklich, dass ein Intervall von 2 Stunden bei Gesundheitsfachpersonen vorgegeben werde. Die Zeitangaben seien zu streichen, oder eine maximale Dauer anzugeben. Ein Timeout nach max. 20 Minuten solle für alle gelten. Die *FMH*, die *SGMI* und die *STSAG* bezeichnen die Definition von Session Timeouts in einer Verordnung als unverhältnismässig und fordern dementsprechend die Streichung von Ziffer 4.21. *Bleuer* macht bezüglich den Bestimmungen unter Ziffer 4.21 auf die Gefahr aufmerksam, dass die Dokumente unvollständig abgerufen werden und daher eine Streichung erfolgen solle resp. zumindest längere Zeiten zu definieren seien. Die *BINT* fordert bezüglich Ziffer 4.21 die Streichung, da unvollständige Daten zur Patientin / zum Patienten die Folge sein können. Bei den eigenen Daten stelle dies einen Eingriff in die Privatsphäre dar. Es stelle sich die Frage, warum das auf Verordnungsebene geregelt wird und weshalb die Zeit für die Patientin / den Patienten kürzer ist. Gemäss der *ISSS* sei es zwar richtig, dass ein Ablauf der Sitzung stattfinden soll, allerdings wäre dieser sinnvollerweise anderswo zu definieren und hier darauf zu verweisen. Es sollte nicht der ganze Anhang angepasst werden müssen, wenn eine Anpassung der Ablaufzeit stattfindet. Ausserdem wäre es womöglich passender, generell von Sitzungen zu sprechen (und nicht von Netzwerk-Sitzungen), da die gleichen Grundsätze auch für offline-Arbeitsplätze gelten können. Sie macht folgenden Formulierungsvorschlag für Ziffer 4.21.1: „[…] definierten Inaktivitätsperiode automatisch beendet werden" und den folgenden für Ziffer 4.21.2: „[…], wenn während der Inaktivitätsperiode keine Interaktion des Benutzers mit dem elektronischen Patientendossier stattfand". *SCH* weist darauf hin, dass die Erfahrungen aus dem Swisscom Gesundheitsportal zeigen, dass eine kurze Session-Dauer als erhebliche Einschränkung der Benutzbarkeit wahrgenommen werde, insbesondere wenn nach Ablauf der Session jeweils eine erneute 2-Faktor-Authentifizierung zwingend ist. Die Limitierung der Session-Dauer sei eine heute übliche Massnahme zur Verhinderung des Session Hijacking. Da der massenhafte Download von Dokumenten des elektronischen Patientendossiers gemäss Verordnung bereits ausgeschlossen ist, sei der erwartete Schaden im Eintrittsfall auf eine einzelne Patientin / einen einzelnen Patienten und auf eine beschränkte Zahl von Dokumenten eingeschränkt. Es sei nicht ausgeschlossen, dass innovative IT-Betreiber andere Verfahren zur Verhinderung von Session Hijacking entwickeln, um damit dem Wunsch nach besserer Benutzbarkeit nachzukommen. Die *SCH* schlägt vor, dass der Betreiber der Gemeinschaften angemessene Massnahmen zur Verhinderung des Session Hijacking nach aktuellem Stand der Technik nachweisen. 6 Kantone[136] geben bezüglich Ziffer 4.21.1 zu bedenken, dass 2 Stunden für eine Gesundheitsfachperson zu kurz seien und 4 Stunden resp. ein halber Tag besser geeignet sei. Es sollte vermieden werden, dass sich eine Ärztin / ein Arzt zu oft neu anmelden muss. Sie fordern konkret, dass die Zeitdauer abgeändert wird und die Klärung des Begriffes „les sessions dans le réseau". Für die *SUVA* ist nicht nachvollziehbar, weshalb inaktive Netzwerk-Sitzungen nach einer definierten Inaktivitätsperiode von 20 Minuten bei Patientinnen / Patienten und 2 Stunden bei den Gesundheitsfachpersonen beendet

[136] FR, NE, GE, VS, VD, JU

werden müssen. Dies sei ein schwerer Eingriff in die Privatsphäre der Patientin / des Patienten, zudem seien die unterschiedlichen Benutzungsdauern weder gesetzeskonform noch sei die Verhältnismässigkeit gewahrt. Ziffer 4.21.1 sei entweder zu streichen, oder eventualiter die gleiche Beschränkungsdauer abzugleichen.

4.22 Zwischenspeicher (Abs. 3)

Das *KSSG* schreibt, dass ein Coaching von solchen Daten möglich sein müsse, damit eine akzeptable Performance des elektronischen Patientendossiers ermöglicht werde bzw. bei einem Ausfall des zentralen Services CPI das elektronische Patientendossier weiter funktioniere.

4.23 Verfügbarkeit (Abs. 3)

Die *ISSS* kritisiert bezüglich Ziffer 4.23.1.2, dass eine „vertraglich vereinbarte Verfügbarkeit über die Zeit von mindestens 98%" eine ungenügende Formulierung sei. Wird 1 Jahr als Massstab genommen, entspräche das 7 Tage Ausfall. Eine Formulierung über einen bestimmten Zeitraum und/oder mittels absolut definierter Ausfalldauer sei vorzuziehen, weshalb folgender Zusatz der Ziffer angefügt werden solle: „[…] Last aufweisen, wobei die maximale Ausfalldauer am Stück 48h nicht überschreiten darf". Eine Präzisierung von Ziffer 4.23.1.2 fordert die *Post*. Sie fragt insbesondere, was „sowie unter Last" bedeute. Zudem müssten diese Anforderungen auch für externe Systeme erfüllt werden, die für die Gemeinschaften relevant sind. Die *Post* beantragt daher, diese Verpflichtung für die ZAS und für Zentrale Dienste am richtigen Ort in den Verordnungen niederzuschreiben. *HIN* weist bezüglich Ziffer 4.23.1.3 darauf hin, dass es keinen vollständigen Schutz gegenüber DoS-Attacken ohne spezifische Endgeräte gebe. Es stelle sich zudem die Frage, wieso genau diese Bedrohung explizit erwähnt wird und andere Bedrohungen nicht. *HIN* geht davon aus, dass die verschiedenen Normen (ISO etc.) einen state-of-the-art Schutz der Internet-Ressourcen implizieren. Als Ersatz wird die Einführung von Service Level Agreements für Cross-Community Anfragen, Patienten / Gesundheitsfachpersonen-Portal, vorgeschlagen. Ziffer 4.23.1.3 sei zu streichen. Zur selben Ziffer schreibt die *Tessaris*, dass sich nach hier vertretener Auffassung ein absoluter Schutz gegen DDoS-Angriffe nicht realisieren lasse. Es sollten jedoch die nach dem Stand der Technik verfügbaren Mittel zur Abwehr solcher Angriffe eingesetzt werden. Es wird folgende Formulierung vorgeschlagen: „[…] des elektronischen Patientendossiers nach dem Stand der Technik gegen sog. DDoS Angriffe geschützt sind". Die *STSAG* sieht in Ziffer 4.23.1.4 einen inadäquaten Aufwand, weswegen die Bestimmung zu streichen sei.

4.24 Datenspeicher unter Schweizer Rechtshoheit (Abs. 4)

Die *privatim* verweisen an dieser Stelle auf ihre Ausführungen zu Artikel 11 Absatz 4 EPDV. Der Kanton *AR* befürwortet die Speicherung der Daten unter Schweizer Hoheitsrecht. Die *GDK* sowie 8 Kantone[137] kritisieren, dass die Vorgaben zur Unterstellung des elektronischen Patientendossiers unter Schweizer Recht nicht überzeugend seien. Es sei zu befürchten, dass damit das Ziel nicht erreicht werden kann, womit Ziffer 4.24 vollständig zu überarbeiten sei. Eine vollständige Überarbeitung fordern auch der *ZAD* sowie die Kantone *ZG* und *ZH*. Sie schreiben, dass die Formulierung „juristische Personen, die unter Schweizer Recht sind" nicht gebräuchlich sei und fragen, was damit gemeint ist. Das Gleiche gelte für die Formulierung: „für die Erbringung der Leistung ausschliesslich unter Schweizer Recht handeln." Diese Garantie dürfte ein Betrieb, der nicht nur in der Schweiz tätig ist, kaum erfüllen können. Es stelle sich die Frage, was diese Formulierung bezweckt. Auch die Formulierung „Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erbringen" sei nicht klar. Sie fragen, was mit einer Firma sei, deren Server in der Schweiz stehen und deren Verwaltung sich in der Schweiz befindet, die aber für einzelne Dienstleistungen auf Anbieter im Ausland zurückgreift (was für die meisten der grösseren Betriebe zutreffen dürfte). Gemäss der *ZAD* und dem Kanton *ZH* sei zudem zu prüfen, ob die Vorgabe, es müsse sich um einen Schweizer Betrieb handeln, mit den Bestimmungen des öffentlichen Beschaffungswesens (insbesondere: Einhaltung des GPA und der bilateralen Verträge) im Einklang steht.

[137] BL, GL, LU, OW, UR, FR, NW, SZ

Die *KKA*, der *BüAeV*, die *GAeSO*, die *KAeG SG* und *HIN* schreiben bezüglich Ziffer 4.24.1.1, dass die Formulierung, wonach sicherzustellen sei, dass der Betrieb der gemeinschaftsinternen Datenspeicher des elektronischen Patientendossiers von juristischen Personen erbracht werde, die „unter Schweizer Recht sind" unklar sei. Es werde vermutet, dass gemeint sei, dass diese juristischen Personen Schweizer Recht unterstehen müssen. Sie geben folgende Formulierungsalternativen: „Schweizer Recht unterstehen", oder „in der Schweiz domiziliert sind". *SCH* gibt zu Ziffer 4.24.1.2 zu Protokoll, dass gemäss Anhang die Leistungen gesamtheitlich der Schweiz erbracht werden müssen. Allein aufgrund der Technologieherrschaft im Ausland seien IT-Lösungen unter ausschliesslicher Beteiligung von Parteien in der Schweiz die Ausnahme. Eine Beschränkung der gesamtheitlichen Leistung auf eine Erbringung innerhalb der Schweizer Landesgrenzen führe dazu, dass die Gemeinschaft die Leistungserbringer für jegliche Datenbearbeitung im Ausland ausdrücklich ermächtigen müsste. Dies sei zur Sicherstellung der Einhaltung schweizerischen Rechts nicht notwendig und gefährde eine stabile Leistungserbringung. Auch bei Speicherung der Daten in Rechenzentren in der Schweiz durch schweizerische Unternehmen sei es im Interesse der Kunden eine Datenbearbeitung durch Sublieferanten oder Mitarbeitende aus dem Ausland zuzulassen. Es sollte darauf abgestellt werden, dass die Hauptleistung im Wesentlichen in der Schweiz erbracht wird. *SCH* schlägt folgende Formulierung von 4.24.1.2 vor: „die Hauptleistung ist im Wesentlichen innerhalb der Schweizer Landesgrenzen zu erbringen".

SWICO verlangt die ersatzlose Streichung von Ziffer 4.24.1.3. Die *Tessaris* schreibt bezüglich dieser Regelung, welche sich an Gemeinschaften wende, die in einem erheblichen Umfang privatrechtlich organisiert sind, nach hier vertretener Auffassung gegen Artikel 3 und Artikel 23 Ziffer 2 des Übereinkommens über das öffentliche Beschaffungswesen SR 0.632.231.422 verstosse, weil nicht in guten Treuen davon ausgegangen werden könne, dass Datenschutz und Datensicherheit beim Betrieb des elektronischen Patientendossiers einer Gemeinschaft nur von einem Unternehmen gewährleistet werden kann, welche sich zur Mehrheit in schweizerischem Eigentum befindet. Sie fordert ebenfalls die Streichung der Ziffer. Der *EHS* und der *VGIch* geben bezüglich den Ziffern 4.24.1.3 und 4.24.1.4 zu bedenken, dass juristische Personen in der Schweiz dem Schweizer Recht unterliegen, und zwar unabhängig von der Ausgestaltung der Eigentümerverhältnisse. Die Ausschreibung einer eHealth-Plattform durch eine Schweizer eHealth-Trägerschaft unterliege GATT/WTO und in einem solchen Fall wären ausländische Anbieter, die in der Schweiz eine Niederlassung haben, zwar zur Teilnahme an der Submission berechtigt, dürften eine solche Plattform jedoch nicht selber betreiben. Sie bezeichnen die beiden Ziffern als unzulässig, da sie gegen übergeordnetes Recht verstossen würden. Die TOZ habe keine solche Regelung zu enthalten. 6 Kantone[138] fragen bezüglich Ziffer 4.24.1.4, ob dies bedeute, dass juristische Personen nur in der Schweiz zu arbeiten haben. Die Ziffer solle umformuliert werden. Die *Post* fragt zu dieser Ziffer, ob sich diese Vorschrift auf die in den Verträgen vereinbarte Leistung bezieht. Falls nein und dies generell gelte, wäre eine Anbieterin, die auch noch Leistungen im Ausland erbringt, ausgeschlossen. Das sei nicht sinnvoll, insbesondere weil die *Post* davon betroffen wäre. Die Übersetzung in Französisch habe zudem eine andere Bedeutung als in Deutsch. Sie bittet um Klärung.

5. Kontaktstelle für Gesundheitsfachpersonen (Art. 12 EPDV)

13 Stellungnehmende[139] wiederholen ihren Kommentar von Ziffer 4.10.2.3 betreffend Ziffer 5.1.2.2. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* begrüssen die Schaffung eines Service-Desk. Allerdings fehle hier eine Regelung dazu, wer die Kosten zur Betreibung des Service-Desk sowie der Hilfestellungen des Service-Desk zu bezahlen hat. Für die Gesundheitsfachpersonen dürften durch den Service-Desk keine zusätzlichen Kosten anfallen, da die Einführung des elektronischen Patientendossiers für sie ohnehin schon sehr kostspielig sei. Sie fordern diesbezüglich folgenden Zusatz für Ziffer 5.1.1: „[…] im Umgang mit dem elektronischen Patientendossier kostenlos unterstützt". Die *STSAG* plädiert dafür, dass die Bestimmung gemäss Ziffer 5.1.1 auf Stammgemeinschaften beschränkt wird, womit in der Formulierung das Wort „Gemeinschaft" mit „Stammgemeinschaft" zu ersetzen sei. 6 Kantone[140] schreiben bezüglich Ziffer 5.1.2.2, dass die Mitarbeitenden dem Berufsgeheimnis unterliegen, weshalb

[138] FR, NE, GE, VS, VD, JU
[139] AR, BL, GDK, GL, LU, OW, UR, SZ, ZG, ZH, ZAD, TI, NW
[140] FR, NE, GE, VS, VD, JU

die Erinnerung, sie seien sorgfältig auszuwählen, nichts bringe und die Ziffer somit gestrichen werden könne. Die Kantone *GE*, *VS*, *VD*, *JU* und *FR* schreiben zudem betreffend Ziffer 5.1.2.4, dass die Dokumentation mit der Software des Marktes technisch nicht möglich sei, weshalb sie die Streichung von „et que l'accès est documenté automatiquement" aus der Ziffer fordern. *HIN* begrüsst betreffend Ziffer 5.1.2.4 die Anforderung, die Remote-Zugriffe zu dokumentieren. Eine automatisierte Dokumentation sollte jedoch nicht zwingend erforderlich sein, womit das Wort „automatisch" gestrichen werden soll. Die *Post* stellt sich bezüglich des Remote-Zugriffes die Fragen, wie über diesen zu informieren resp. einzuwilligen sei und wie die Dokumentation darüber erfolgen müsse.

6. Information der Patientin oder des Patienten (Art. 14 EPDV)

Gemäss der *K3*, dem *VZK*, dem *ZAD* sowie den Kantonen *ZG* und *ZH* würden sich die Regelungen gemäss Ziffer 6 bereits aus dem EPDG und dem EPDV ergeben, weshalb sie weggelassen werden können.

6.1.2 / 6.1.3: 6 Kantone[141] sind der Meinung, dass die Punkte, die den Patientinnen / Patienten zu erklären sind, zu lang und zu kompliziert seien, um von ihnen verstanden zu werden. Die Erfahrung der Kantone aus der Romandie, welche auf mehr als zehntausend Patientinnen / Patienten besteht, zeigt, dass die Konzentrations- und Geduldszeit einer Patientin / eines Patienten nicht mehr als 15 Minuten betrage. Nur die wesentlichen Punkte müssen erklärt werden. Gemäss ihren praxisbasierten Schätzungen würde es mindestens 30 zusätzliche Minuten brauchen, um die Punkte der Ziffer 6.1 einer Person im mittleren Alter mit körperlicher Gesundheit zu erklären. Für eine Gemeinschaft mit 100'000 Patientinnen / Patienten, würde es 4'500'000 Minuten brauchen, d.h. 9'375 Manntage oder 42 Mannjahre. Mit 10 Mitarbeitenden (d.h. 1 Mio CHF/Jahr Löhne), würde es 4 Jahre brauchen. Es wird gefordert, dass in erster Linie nur die folgenden Punkte angenommen werden: 6.1.2.5, 6.1.3.5, 6.1.4.1-2-5, 6.1.5.2. Die Patientin / der Patient müsse die Möglichkeit haben, sich über die weiteren Themen zu informieren. Der *VAKA*, die *K3* und der *VZK* schreiben, dass die Informationen gemäss Ziffer 6.1.2.1 wohl jede normale Patientin / jeden normalen Patienten überfordern würden, weshalb die Ziffer zu streichen sei. Weiter fügt der *VAKA* betreffend Ziffer 6.1.2.3 an, dass dies jede Stammgemeinschaft im eigenen Interesse tue und somit nicht vorgeschrieben werden müsse resp. ebenfalls zu streichen sei. Das *KSSG* gibt bezüglich Ziffer 6.1.3.2 zu bedenken, dass die Stammgemeinschaft die Patientin / den Patienten zwar darüber informieren könne, jedoch keine Möglichkeit habe, dies sicherzustellen. Gemäss der *OFAC* sei es nötig zu präzisieren, dass man von einem einzigen Patientendossier gemäss EPDG redet. Dieses sei in einer zertifizierten Stammgemeinschaft beherbergt, die einen einzigen PID benutze, der von der ZAS generiert ist. Dazu würden die kantonalen Pilot-Dossiers, die nach den EPDG-Anforderungen nicht zertifiziert seien, sowie die Dossiers, die sich nicht auf den einzigen PID beziehen, nicht in Frage kommen. Die *SPO* stellt bezüglich Ziffer 6.1.3.4 die Frage, was mit den beim Wechsel der Stammgemeinschaft verbundenen Konsequenzen gemeint sei. Falls es sich dabei um die in den Ziffern 8.4.2.2 und 8.4.2.3 aufgeführten Prozesse handle sei keine Änderung nötig, ansonsten seien die Konsequenzen einzeln aufzuführen. Der *VAKA*, die *K3* und der *VZK* sehen in Ziffer 6.1.3.5 einen Widerspruch zu der geforderten Aufbewahrung der Widerrufserklärung, was eine Anpassung nötig mache. Die *IG eHealth* schreibt bezüglich Ziffer 6.1.3.6, dass das elektronische Patientendossier gemäss Artikel 20 Absatz 1 EPDV aufgehoben werden könne. Bei der Aufhebung werde die PID in der Identifikationsdatenbank der ZAS annulliert. Nach einem Widerruf zur Führung eines elektronischen Patientendossiers bestehe für eine Patientin / einen Patienten jedoch die Möglichkeit, erneut ein Dossier zu eröffnen. Bei einer Neueröffnung werde eine neue PID zugeordnet. Die *IG eHealth* begrüsst die Möglichkeit für Patientinnen / Patienten, mehrmals ein elektronisches Patientendossier eröffnen zu können. Die Patientin / 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 müsse sie / er die gewünschten Dokumente erneut in seinem elektronischen Patientendossier abspeichern.

6.1.4 / 6.1.5: Die *Post* bittet bezüglich Ziffer 6.1.4.6 zu klären, wie die Erlaubnis für den Remote-Zugriff

[141] FR, NE, GE, VS, VD, JU

eingeholt werden müsse und wie dieser Zugriff zu dokumentieren sei. Gemäss dem Kanton *ZH* und der *ZAD* sei es problematisch vorzusehen, dass Mitarbeitende des Service-Desk einen Remote-Zugriff auf die Endgeräte von Patientinnen und Patienten haben. Sicherheitsmässig korrekt durchgeführte Remote-Zugriffe dürften ohne Beteiligung der Patientin / des Patienten nicht möglich sein. Eine Stammgemeinschaft könne nicht gewährleisten, dass ein solcher Zugriff möglich ist, auf was auch die *K3* und der *VZK* hinweisen. Der Kanton *ZH*, der *ZAD*, die *K3* und der *VZK* fordern dementsprechend die Streichung der Ziffer 6.1.4.6. Der *VGIch* wiederholt seine Stellungnahme von Artikel 14 Absatz 2 EPDV bezüglich Ziffer 6.1.5. Die *STSAG* wünscht eine ergänzende Ziffer 6.1.5.6 mit folgender Formulierung: „das Risiko durch Einstellung der Zugriffsrechte die Behandlungssicherheit zu gefährden und eine allfällige Verantwortung hierfür zu tragen".

7. Einwilligung (Art. 15 EPDV)

Die *K3*, der *VZK* sowie die Kantone *ZH* und *ZG* wiederholen an dieser Stelle ihre Stellungnahme von Ziffer 6. *SCH* fordert, dass im Sinne des Ziels, eine grösstmögliche Digitalisierung zu erreichen, die der Schriftlichkeit gleichgesetzte qualifizierte elektronische Signatur gemäss Artikel 14 Absatz 2bis OR unmissverständlich zu akzeptieren sei. Darüber hinaus sollten auch andere Hilfsmittel zur eindeutigen Identifizierung von Personen zugelassen werden. Die Präzisierung sollte auf Verordnungsstufe klar ausformuliert werden (und nicht erst in den Erläuterungen). Ziffer 7.1.1 sei daher mit folgendem Satz zu ergänzen: „[…] eingeholt wird. Der eigenhändigen Unterschrift gleichgesetzt sind die qualifizierte elektronische Signatur sowie andere Hilfsmittel zur eindeutigen Bestimmung der Identität der Patientin oder des Patienten".

8. Verwaltung (Art. 16 EPDV)

Der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* bezeichnen Ziffer 8 als zu ausführlich und fordern eine Vereinfachung. Grösstenteils würden sich diese Regelung bereits aus dem EPDG und der EPDV ergeben und seien daher zu streichen. Dies gelte insbesondere für die Ziffern 8.6 und 8.7.

8.1 Eintritt und Austritt von Patientinnen und Patienten (Abs. 1 Bst. a)

Die *Post* weist darauf hin, dass der Satz von Ziffer 8.1.1.1 unvollständig scheine und wie folgt zu korrigieren sei: „[…] zur Sicherstellung der Vorgaben nach […]".

8.2 Identifikation der Patientinnen und Patienten (Abs. 1 Bst. b)

Gemäss der *K3* und dem *VZK* gehe die Auflage, dass Patientinnen und Patienten für den Zugriff auf ihr eigenes elektronisches Patientendossier dieselben hohen Anforderungen an die IDM erfüllen müssen wie für Gesundheitsfachpersonen, zu weit. Dies würde bedeuten, dass alle Patientinnen / Patienten ein kostenpflichtiges IDM beschaffen (und erneuern) müssen, damit ihr elektronisches Patientendossier geführt werden könne. Für die Patientinnen / Patienten sollte der Zugriff kostenlos und mit vergleichbaren Mitteln, wie z.B. Online Banking, machbar sein. Die gelte neben der Ziffer 8.2.2 auch für die Ziffer 8.3.1 und je nach Situation für die Ziffer 8.8.2. Die *Post* weist bezüglich Ziffer 8.2.2.1.1 darauf hin, dass sie die AHVN13 haben müsse, damit beim ZAS die PID abgefragt werden könne. Ihrer Meinung nach habe kein Herausgeber eines IDM das Recht die AHVN13 zu erfassen und heraus zu geben. Die ganzen Regeln rund um die Nutzung der IDM seien nicht zielführend. Die *OFAC* wiederholt ihre Stellungnahme von Ziffer 6.1.3.2 und das *KSSG* ihre Bemerkung von Ziffer 6.1.3.2 bezüglich Ziffer 8.2.2.2. Das *KSSG* verlangt zudem entweder die Streichung der Ziffer, oder dass eine technische Möglichkeit zur Abfrage geboten wird. Die *Integic* wünscht eine Klarstellung, wie die Bestimmung von Ziffer 8.2.2.2 sichergestellt werden soll.

8.3 Identifikation und Authentisierung (Abs. 1 Bst. c)

Gemäss dem *VAKA*, der *K3* und dem *VZK* müsse bei Ziffer 8.3.3 unbedingt erwähnt werden, dass eine Authentisierung mittels mTan möglich ist. *HIN* macht nochmals darauf aufmerksam, dass die verlangte,

starke 2-Faktor-Authentisierung begrüsst werde und Ziffer 8.3.3.1 somit so belassen werden sollte. Die *Post* schreibt, dass Ziffer 8.3.3.1 unverständlich sei. Zuerst benötige man ein IDM eines zertifizierten Herausgebers und dann können beliebige Authentifizierungsverfahren eingesetzt werden. Es wird ein Standard gefordert, der für alle gilt.

8.4 Wechsel der Stammgemeinschaft (Bst. e)

Die *privatim* sind der Meinung, dass unter Ziffer 8.4.2 auch festzuhalten sei, dass die „alten" Stammgemeinschaften verpflichtet sind, alle zum elektronischen Patientendossier vorhandenen Informationen zu vernichten – mit Ausnahme der vom Gesetz zur Aufbewahrung vorgesehenen Unterlagen (z.B. Art. 20, Abs. 2, Bst. a EPDV). Konkret machen sie folgenden Formulierungsvorschlag: „alle im Zusammenhang mit dem elektronischen Patientendossier stehenden Daten unwiderruflich vernichtet werden. Ausgenommen sind Unterlagen, die von Gesetzes wegen aufzubewahren sind". Die *Medgate* weist darauf hin, dass Ziffer 8.4.2.2 einen Fehler im Text habe und schlägt folgende Korrektur vor: „die Ermächtigung von Gesundheitsfachpersonen gemäss […]". Die *BFH* bezeichnet es bezüglich Ziffer 8.4.2.3 als nicht ganz einleuchtend, warum Stellvertreter bei einem Wechsel der Stammgemeinschaft das Stellvertreterrecht automatisch verlieren. Dies sollte der Patientin / dem Patienten aktiv mitgeteilt werden. Die Kantone *GE*, *VS*, *VD*, *JU* und *FR* schreiben, dass die Aufhebung des elektronischen Patientendossiers im Falle eines Wechsels der Stammgemeinschaft möglich, aber nicht obligatorisch sein müsse. 6 Kantone[142] schreiben, dass eine Ärztin / ein Arzt, die / der die Patientin / den Patienten verlässt, den Zugriff auf die Krankenakte behält, auch wenn sie / er diese nicht mehr benötige. Zudem gebe es gemäss diesen Kantonen keinen Grund zu glauben, dass eine Patientin / ein Patient, die / der eine Gemeinschaft wechselt, ihre / seine Stellvertreterinnen / Stellvertreter austauschen wolle. Die Ziffern 8.4.2.2 und 8.4.2.3 seien zu streichen. Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* begrüssen, dass, wie in der Vernehmlassung zum EPDG angeregt, eine Regelung zum Wechsel der Stammgemeinschaft aufgenommen wurde. Es sei allerdings fraglich, ob der Wechsel der Stammgemeinschaft mit den festgelegten Regeln auch funktioniere, wenn eine Stammgemeinschaft aufgelöst wird und was passiert, wenn die Stammgemeinschaft den Umzug nicht vornehmen kann. Es wird angeregt, dass hier die Verpflichtung zur Statuierung einer Auffangregelung aufgenommen wird. Sie fordern eine neue Ziffer 8.4.2.4 mit folgender Formulierung: „der Wechsel der Stammgemeinschaft auch dann möglich ist, wenn die Stammgemeinschaft den Wechsel nicht durchführen kann".

8.5 Durchsetzen der Zugriffsentscheidung zur Bearbeitung der Berechtigungskonfiguration (Abs. 2: Zugriffsrechte (Art. 2 EPDV Abs. 1) und Optionen der Patientinnen und Patienten (Art. 3 EPDV)

Das *KSSG* kritisiert, dass die Formulierung von Ziffer 8.5.1 unverständlich sei und nicht interpretiert werden könne. Die Ziffern 8.5 und 8.5.1 seien dementsprechend so zu formulieren, dass die Anforderungen verständlich und klar seien.

8.6 Berechtigungssteuerung (Abs. 2): Zugriffsrechte (Art. 2 EPDV Abs. 1 bis 4)

Gemäss dem *VAKA* sei unklar, worin der Mehrwert dieser Ziffer bestehe. Sie bilde doch nur die Infos aus der EPDV ab und sollte daher gestrichen werden. Die *BFH* verweist bezüglich Ziffer 8.6.2.3 auf ihren Kommentar zu der Problemstellung rund um Artikel 8 Buchstabe e EPDV.

8.7 Optionen der Patientinnen und Patienten (Art. 3 EPDV)

Der *VAKA* wiederholt an dieser Stelle seine Stellungnahme zu Ziffer 8.6. Der Kanton *AR* verweist bezüglich Ziffer 8.7.2.1 auf die Kommentare und Änderungsvorschläge zu Artikel 3 Buchstabe a EPDV. Das *KSSG* weist darauf hin, dass im Spital vor allem die Assistenzärztinnen / Assistenzärzte relativ oft den Fachbereich und somit die Gruppe wechseln würden. Ziffer 8.7.2.6 würde gerade den Assistenzärztinnen / Assistenzärzten, welche am meisten auf die Daten des elektronischen Patientendossiers angewiesen seien, den Zugriff auf relevante Informationen verbieten. Sie sei deshalb zu streichen. Es

[142] FR, NE, GE, VS, VD, JU

reiche, wenn die Patientin / der Patient über neu eintretende Personen und Mutationen informiert wird. Die *Post* schreibt bezüglich Ziffer 8.7.2.8, dass dies eine Standardeinstellung sein sollte. Es sei zu klären, wie weit die Berechtigungskette geht. 6 Kantone[143] erachten Ziffer 8.7.2.9 als unklar und wünschen die Aufführung von konkreten, klärenden Beispielen.

8.8 Stellvertretung (Art. 16 Abs. 3)

Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* schreiben, dass Artikel 16 Absatz 3 EPDV nicht existiere. Der entsprechende Verweis im Titel sei daher zu streichen und allenfalls durch Artikel 3 Buchstabe g EPDV zu ersetzen. 6 Kantone[144] weisen darauf hin, dass in der französischen Version bei den Ziffern 8.8.2 und 8.8.3.4 zweimal das Wort „du patient" geschrieben wurde, womit es bei beiden Ziffern einmal zu streichen sei. Bezüglich Ziffer 8.8.3.4 fügen sie an, dass die Stellvertretung mehrere Authentisierungsmittel (mTan, SwissID, etc.) haben könne. Zudem schreiben sie, dass es in der Praxis schwierig sein werde, im Zuge eines Zertifizierungsaudits die Realisierung dieser Anforderung sicherzustellen. Des Weiteren seien konkrete Beispiele bezüglich der Art dieser „eindeutigen und konkreten" Sicherstellung anzugeben. Sie fordern folgende Formulierung von Ziffer 8.8.3.4: „le compte utilisateur servant au représentant du patient est relié de manière […]".

9. Zugangsportal für Patientinnen und Patienten (Art. 17 EPDV)

9.1 Konformität mit gesetzlichen Bestimmungen

9.1.1: Der *VAKA* schreibt bezüglich Ziffer 9.1.1, dass es sich wohl um einen fehlerhaften Eintrag handle und verlangt die Streichung. Die *Post* fragt, was mit „einschlägig rechtlichen Anforderungen" gemeint sei und fordert eine Präzisierung von Ziffer 9.1.1. Ähnlich schreiben die *privatim*, dass unklar sei, auf welche einschlägigen gesetzlichen Bestimmungen Bezug genommen werde. Der Wortlaut solle präzisiert und einige der Bestimmungen genannt werden. Gemäss den Kantonen *ZG* und *ZH*, der *K3*, dem *VZK* und dem *ZAD* sei es selbstverständlich, dass die einschlägigen rechtlichen Bestimmungen eingehalten werden müssen. Das gelte ohnehin. Es sei falsch, dies als Zertifizierungsvoraussetzung zu verlangen. Eine Zertifizierungsstelle sei nicht in der Lage zu prüfen, ob alle Bestimmungen eingehalten werden. Ziffer 9.1.1 sei zu streichen.

9.1.3: 6 Kantone[145] bezeichnen Ziffer 9.1.3.1 als unklar. Wenn die Patientin / der Patient die Daten zur Verfügung stellt, stimme sie / er zu. Der Sachverhalt müsse geklärt werden. Die *Medgate* weist bei derselben Ziffer auf folgenden Schreibfehler hin: „[…] nur dann im elektronischen Patientendossier erfasst […]". Die *Post* macht geltend, dass sich die Ziffern 9.1.3.1 und 9.1.3.2 widersprechen. Es gebe Dokumente die ausserhalb des elektronischen Patientendossiers erfasst werden und bei der Übertragung ins Dossier die Einwilligung der Patientin / des Patienten benötigen. Andererseits sei es verboten, Dokumente ausserhalb des Dossiers zwischen zu speichern. Es sei eine Präzisierung nötig. *SBC* ist der Meinung, dass die Limitation gemäss Ziffer 9.1.3.2 keinen Sinn mache und fordert die Streichung der Ziffer. Ebenfalls die Streichung fordert die *SGMI*. Sie schreibt, dass die Erfassung der von der Patientin / dem Patienten bereitgestellten Daten immer nur direkt im elektronischen Patientendossier unverhältnismässig sei. Gemäss der *BINT* sei Ziffer 9.1.3.2 zudem nicht sinnvoll als generelle Regel, womit ebenfalls die Streichung gewünscht wird. Ob ein Dokument direkt ins elektronische Patientendossier hochgeladen und danach in einen anderen Speicher heruntergeladen wird oder umgekehrt, spiele keine Rolle. Die *Medgate* macht auch bei dieser Ziffer einen Schreibfehler geltend. Es müsse „bereitgestellten" geschrieben werden. Für die *privatim* stellt sich hier die Frage, wie mit Daten zu verfahren sei, die mittels Gesundheits-Apps ins elektronische Patientendossier gelangen sollen. Sie fragen, wie sichergestellt werde, dass diese Daten nicht mit Malware oder ähnlichem versehen sind. Die *OFAC* gibt betreffend Ziffer 9.1.3.3 zu bedenken, dass diese den Ziffern 3.5.1.3 und 9.5.1.3, welche den „bulk download"

[143] FR, NE, GE, VS, VD, JU
[144] FR, NE, GE, VS, VD, JU
[145] FR, NE, GE, VS, VD, JU

autorisieren, widerspreche. Für 6 Kantone[146] ist zudem der Sinn des Satzes bei Ziffer 9.1.3.3 unklar. Es solle erklärt werden, was mit „funktionelle Bereiche“ gemeint sei. Die *SGMI* weist darauf hin, dass die Patientin / der Patient die Weitergabe von Daten über die Berechtigungsvergabe steuern könne. Es könne sehr wohl im Sinne der Patientinnen / Patienten sein, dass ihre / seine erfassten Daten implizit weitergeleitet werden. Ziffer 9.1.3.3 sei dementsprechend zu streichen. Die *FMH* verlangt im Sinne der Patientenbehandlung und -sicherheit eine kritische Prüfung der Vorgaben von Ziffer 9.1.3.3.

9.2 Darstellung

12 Stellungnehmende[147] wiederholen ihre Kommentare von Ziffer 3.2.1.3 bezüglich Ziffer 9.2.1.3. Die *BFH* schreibt, dass der Unterschied zwischen den Ziffern 9.2.1.1 und 9.2.1.2 nicht klar sei. Die *Medgate* macht auf 2 Schreibfehler aufmerksam. Bei Ziffer 9.2.1.1 müsse „Gesundheitsfachperson“ anstatt „Gesundheitsfachpersonen“ geschrieben sein und bei Ziffer 9.2.1.5 „Zugriffsrechte“ anstatt „Zugriffsrechten“.

9.3 Barrierefreiheit

Der *VAKA*, die *K3* und der *VZK* weisen bezüglich Ziffer 9.3.1.1 darauf hin, dass sich Barrierefreiheit auf Menschen mit Behinderungen und nicht auf ältere Menschen beziehe. Zudem regen sie an, den Begriff „behinderte Patientinnen und Patienten“ durch „Menschen mit Behinderung“ zu ersetzen. Konkret schlagen sie die Streichung der Wörter „behinderte oder ältere“ aus der Ziffer vor. 6 Kantone[148] verweisen bezüglich Ziffer 9.3 auf die relevanten Stellungnahmen von Ziffer 3. Der *SBV* wiederholt zudem seine Stellungnahme von Ziffer 3.3.1.2 bezüglich Ziffer 9.3.1.2. Der *VGIch* schreibt, dass die Grundzüge der Anforderung in der Verordnung zu regeln seien und nicht erst in der EDI-Ausführung. Dem Legalitätsprinzip werde hier nicht entsprochen.

9.4 Dateiformate: Bereitstellung

6 Kantone[149] verweisen bezüglich Ziffer 9.4 auf die relevanten Stellungnahmen von Ziffer 4. Der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* schreiben, dass sich die Regelungen von Ziffer 9.4 bereits aus dem EPDG und der EPDV ergeben würden oder selbstverständlich und damit zu streichen seien. *SCH* wiederholt ihre Stellungnahme von Ziffer 3.4 bezüglich Ziffer 9.4 und die *K3* sowie der *VZK* ihren Kommentar von Ziffer 3.4.1.2 betreffend Ziffer 9.4.1.2. Die *Post* schreibt bezüglich Dateiformaten, dass die EPDV-EDI Anhang 4 als Quelle definiere, die TOZ wiederum Anhang 3 (Metadaten), was eine Präzisierung nötig mache. Es könne zudem nicht sein, dass das elektronische Patientendossier zum Dokumentenkonverter verordnet wird. Konvertierung zu PDF beim Benutzer oder Primärsystem sei heute kein Problem mehr. Die *Post* ist der Meinung, dass keine Dokumente umgewandelt werden müssen und beantragt, diese Forderung zu löschen.

9.5 Dateiformate: Abruf

Der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* wiederholen ihre Stellungnahme von Ziffer 9.4. 6 Kantone[150] verweisen bezüglich Ziffer 9.5 auf die relevanten Stellungnahmen von Ziffer 5. Die *BFH* fragt, weshalb das Zugangsportal den Download in ein Primärsystem unterstützen müsse. Die Gesundheitsfachperson habe ja einen eigenen Zugang. Ziffer 9.5.1.2 sei allenfalls zu streichen. *SCH* weist bezüglich dieser Ziffer darauf hin, dass die Patientin / der Patient kein Primärsystem besitze. Ähnlich fragt die *Medgate*, was hier mit Primärsystem gemeint sei und vermutet, dass es sich um einen Fehler handle, was zu korrigieren sei. Die *Post* schreibt, dass die Forderung gemäss Ziffer 9.5.1.3 nicht nachvollziehbar sei. Wie die Schnittstellen innerhalb von Gemeinschaften funktionieren sei „out of scope“ für das EPDG

[146] FR, NE, GE, VS, VD, JU
[147] FR, BL, GDK, GL, LU, OW, UR, SBC, NW, SZ, TG, VGIch
[148] FR, NE, GE, VS, VD, JU
[149] FR, NE, GE, VS, VD, JU
[150] FR, NE, GE, VS, VD, JU

und zwischen den Gemeinschaften würden die Vorgaben von XCA (oder XCF) gelten. Diese Forderung mache nur dann Sinn, wenn auch standardisiert wird, wie ein „bulk download" gemacht werden kann. Es wird beantragt diese Forderung zu löschen. Des Weiteren gibt die *Post* zu bedenken, dass die rate limits und entsprechende use cases detailliert definiert werden müssen. Ansonsten bestehe das Risiko von endlosen Diskussionen. Auch hier wird die Löschung der Forderung gewünscht.

9.6 Protokolldaten (Bst. c)

Der Kanton *ZH*, die *K3*, der *VZK* und der *ZAD* wiederholen ihre Stellungnahme von Ziffer 9.4 und 9.5. Die *BFH* fragt, was mit „lesbarer Form" gemeint sei und schlägt alternativ folgendes Wording vor: „[…] allen Gemeinschaften und Stammgemeinschaften in einem für sie nachvollziehbarem, eindeutig und leicht verständlichem Inhalt einzusehen". Die *privatim* bemängeln, dass aus dieser Formulierung nicht hervorgehe, inwiefern eine Patientin / ein Patient eine Gesamtübersicht aller Protokolldaten aus allen Gemeinschaften und Stammgemeinschaften erstellen kann. Dies sei für eine effektive Kontrolle jedoch wichtig. Es sei zu prüfen, inwiefern der Wortlaut in diese Richtung präzisiert werden könne.

10. Verfügbarkeit der von Patientinnen und Patienten erfassten Daten (Art. 18 EPDV)

10.1 Dokumentenablagen für Dokumente von Patientinnen und Patienten

10.1.1 / 10.1.2: *HIN* geht davon aus, dass mit „dezidiert" gemäss Ziffer 10.1.1 keine physische Trennung gemeint ist. Eine logische Trennung reiche völlig. Es wird folgender Zusatz vorgeschlagen: „[…] bereitstellen, die von den Dokumentenablagen für die Gesundheitsfachpersonen und Gesundheitseinrichtungen logisch getrennt sind". Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* schreiben, dass die Dokumentenablage für die durch Patientinnen und Patienten selbst erfassten Daten unbedingt separat von der Dokumentenablage der Gesundheitsfachpersonen und Gesundheitseinrichtungen zu führen sei, damit die entsprechenden Dokumente bereits durch deren Ablageort klar voneinander unterschieden werden können und damit die Behandlungssicherheit gewährleistet bleibe. Ähnlich wie die *HIN* fordern sie folgenden Zusatz für Ziffer 10.1.1: „bereitstellen, die von den Dokumentenablagen für die Gesundheitsfachpersonen und Gesundheitseinrichtungen getrennt sind". Das *KSSG* macht darauf aufmerksam, dass eine Trennung der Repositories für die durch die Patientin / den Patienten eingestellten Dokumente und der durch die Gesundheitsfachpersonen eingestellten Dokumente die Wartungs-, Lizenz- und Betriebskosten von einem Repository verdopple. Eine Trennung könne auch auf logischer Ebene erfolgen. Die Ziffer 10.1.1 sei zu streichen. 6 Kantone[151] kritisieren, dass die Übersetzung von Ziffer 10.1.1 mangelhaft sei und fordern folgende Anpassung bei der Formulierung: „[…] des lieux de stockage dédiés […]" Bezüglich Ziffer 10.1.2 fordern die Kantone zudem folgende Anpassung: „[…] à aucun effacement". Die *OFAC* fragt bezüglich Ziffer 10.1.2, ob die Daten nicht den gleichen Regeln wie diejenigen unter Ziffer 2.1.1.1 unterliegen. Durch die übermässige Aufbewahrung entstünden unnötige Risiken und es sei ein Verstoss gegen den Grundsatz der Verhältnismässigkeit des DSG.

10.1.3 / 10.1.4: Die *BFH* gibt bezüglich Ziffer 10.1.3 zu bedenken, dass 2 GB viel sei, wenn es um Textdokumente gehe, allerdings weniger, wenn es darum gehe Vitaldaten zu erfassen und gar nichts, wenn es darum gehe, Bilder hochzuladen. Der heute gängige zur Verfügung stehende Speicherplatz liege eher bei 10 GB als bei 2, daher sollte von marktüblichen, aber mindesten 10 GB Speicherplatz gesprochen werden. *PharmaSuisse* ist der Meinung, dass 2 GB zu wenig seien und empfiehlt eine Mindestgrösse von 5 GB, wie dies bei kostenlosen Cloud-Diensten üblich sei. Für 17 Stellungnehmende[152] erscheint die verlangte Grösse des Speicherplatzes von 2 GB als willkürlich, weshalb diese Bestimmung zu streichen sei. Es solle eine generell-abstrakte Regelung in die EPDV aufgenommen werden, wonach das elektronische Patientendossier so viel Platz bietet, dass Patientinnen und Patienten alle relevanten Dokumente ablegen können. 6 Kantone[153] geben zu bedenken, dass 2 GB bei weitem nicht ausreichend seien, um die Bedürfnisse gewisser Patientinnen / Patienten abzudecken und

[151] FR, NE, GE, VS, VD, JU
[152] GDK, BL, GL, LU, OW, UR, ZG, ZH, SZ, TG, AR, NW, K3, VZK, SGMI, FMH, ZAD
[153] FR, NE, GE, VS, VD, JU

fordern folgende Formulierung von Ziffer 10.1.3: „Les communautés doivent garantir et s'organiser pour fournir un espace de stockage correspondant au besoin". Zudem sei Ziffer 10.1.4 zu streichen.

10.2 Offline-Archivierung von Dokumenten und Metadaten

Die *Post* und der *VAKA* schreiben, dass die Regeln zum reimportieren von Dokumenten keinen wirklichen Use Case zu haben scheinen, aber sie würden relativ viel Kosten verursachen, weil diese Technologie weder vorhanden, wohl aber auch noch sehr aufwendig sein werde. Ziffer 10.2 sei ersatzlos zu streichen. Die *OFAC* fragt u.a., welchem Zweck die Bestimmungen dieser Ziffer dienen und ob sie gratis seien. Sie gibt zu bedenken, ob nicht unnötige Risiken entstehen, wenn eine schlecht sensibilisierte Patientin / ein schlecht sensibilisierter Patient ihr / sein Archiv offline auf einem Cloud-Markt platziere.

Gemäss der *Post* sollte, wenn Interoperabilität gefordert wird, auch spezifiziert werden, wie die Formate aussehen. Ziffer 10.2.1 sei entweder zu streichen oder Spezifikationen nach zu liefern. Die *BFH* fragt, ob mit patientenbezogenen Daten hier nur die administrativen Daten gemeint seien, oder ob Behandlungsdaten auch dazu gehören würden. Es wird darauf hingewiesen, dass dafür noch keine interoperablen Formate spezifiziert worden seien, zumindest wenn bei dem Wort Interoperabilität nicht ein PDF gemeint sein solle. Es sei genauer zu spezifizieren, welche patientenbezogenen Daten gemeint sind. *Economiesuisse* und *SBC* schlagen vor, dass Ziffer 10.2.1 für alle Daten der Patientin / des Patienten gelten solle und nicht nur für die von der Patientin / dem Patienten erfassten Daten, die das Thema von Ziffer 10 seien. Allenfalls müsse der Titel von Ziffer 10 folgendermassen angepasst werden: „ […] oder Patienten und Gesundheitsfachpersonen erfassten […]". *HIN* schreibt, dass analog Ziffer 3.4.1.2 davon ausgegangen werde, dass die Forderung gemäss Ziffer 10.2.1 ausreichend erfüllt sei, wenn nicht akzeptierte Formate gar nicht erst eingestellt werden können.

SCH weist darauf hin, dass die Verordnung keine Formate oder Transaktionen vorschreibe und damit einen grossen Spielraum für proprietäre Implementierungen zulasse, welche unkalkulierbar hohe Aufwände für den konsistenten Import nach sich ziehen können. IHE definiere im technischen Framework (ITI-32 Portable Media Creator und Importer) bereits die Akteure, Transaktionen sowie Formate für den Import und Export der Daten und Dokumente aus der Registry und den Repositories in IHE konformen Gemeinschaften. Dabei beziehe sich die Spezifikation auf entsprechende Use Cases im Bereich DICOM und verweise in den wesentlichen Punkten auf den DICOM Standard. Die IHE Spezifikation beschreibt bereits auch die Berechnung von Hash Werten der Daten und Dokumente zur Sicherstellung der Integrität und des originalen Zustands. *SCH* fordert folgende Neuformulierung der 3 Ziffern unter Ziffern 10.2 in neu 2 Ziffern: „10.2.1 Gemeinschaften müssen den Patienten und Patientinnen die Möglichkeit zum Export und Import der Daten und Dokumente ihres elektronischen Patientendossiers im interoperablen elektronischen Format gemäss IHE iti-32 zur Verfügung stellen; 10.2.2 Stammgemeinschaften müssen mit den in IHE iti-32 definierten Verfahren sicherstellen, dass Daten, die erneut im elektronischen Patientendossier verfügbar gemacht werden sollen, unverändert geblieben sind.

Die *K3* und der *VZK* kritisieren bezüglich den Ziffern 10.2.2 und 10.2.3, dass diese kaum umfassend zu realisieren seien, da Patientinnen und Patienten Dokumente herunterladen, löschen und verändert wieder hochladen können. Somit seien die beiden Ziffern zu streichen. Ähnlich schreiben 6 Kantone[154] zu denselben Ziffern, dass es ohne ein System, welches für jedes Dokument eine vollständige Rückverfolgung generiert, nicht möglich sei festzustellen, ob Daten verändert wurden. Sie wünschen ebenfalls die Streichung der Ziffern 10.2.2 und 10.2.3. Die *Integic* plädiert dafür, dass die Ziffern unter 10.2 weiter ausgeführt werden, da sie missverständlich seien. Insbesondere Ziffer 10.2.3 sei z.B. bei Ergebnissen der bildgebenden Diagnostik (DICOM) evtl. problematisch. Offline-Archivierung müsse sich immer auf das ganze Dossier beziehen. Wenn ein Teilnehmender aus einer Gemeinschaft ausscheidet, sollte das die Patientin / den Patienten nicht kümmern. Ggf. habe die Stammgemeinschaft die dort gelagerten Daten zu übernehmen. Das *KSSG* bemängelt, dass eine solche Überprüfung auf den bestehenden IHE-Profilen nicht umsetzbar sei. Wird ein Dokument erneut registriert, dann werde eine neue Unique Document ID erstellt und mit dieser registriert. Eine Deduplizierung von Dokumenten (prüfen des Hash, etc.)

[154] FR, NE, GE, VS, VD, JU

sei keine IHE Funktionalität. Das *KSSG* fordert die Streichung von Ziffer 10.2.3. Die *OFAC* fordert eine Erklärung, was mit „erneut im elektronischen Patientendossier verfügbar gemacht werden sollen“ gemeint sei.

11. Kontaktstelle für Patientinnen und Patienten (Art. 19 EPDV)

Die *KKA*, der *BüAeV*, die *GAeSO* und die *KAeG SG* begrüssen die Schaffung eines Service-Desk für Patientinnen / Patienten. Es sei jedoch keine Regelung darüber getroffen worden, wer die Kosten des Service-Desk zu tragen habe. Dies müsse ergänzt werden. Für die Gesundheitsfachpersonen dürfen durch diesen Service-Desk keine zusätzlichen Kosten anfallen, da die Einführung des elektronischen Patientendossiers für sie ohnehin schon sehr kostspielig sei. Der *VGIch* schreibt bezüglich Ziffer 11.1.1, dass die gleichen Vorgaben zur Protokollierung wie bei den Kontaktstellen Gesundheitsfachpersonen gelten. Hier seien Lücken in der Verordnung feststellbar bzw. Undeutlichkeiten in den Erläuterungen. Durchgängigkeit sei sicherzustellen. Zugriffe seien von allen zu protokollieren. Weiter wird darauf hingewiesen, dass die ärztliche Schweigepflicht eine strafrechtliche Bestimmung sei, welche nicht mit einer „analogen Vereinbarung“ gemäss Ziffer 11.1.2.2 übertragen werden könne. Bezüglich Ziffer 11.1.2.4 fordert der *VGIch* zudem folgende Anpassung im Erlasstext: „[…] Einwilligung der jeweiligen Patienten erfolgen können […]“. Ähnlich spricht die *Medgate* von einem inhaltlichen Fehler und fordert folgende Korrektur: „[…] Einwilligung der jeweiligen Patientin oder des jeweiligen Patienten erfolgen können […]. Die *privatim* geben zu bedenken, dass nicht nachvollziehbar sei, weshalb eine Gesundheitsfachperson ihre Einwilligung für Remote-Zugriffe auf Endgeräte der Patientin / des Patienten geben müsse. Für entsprechende Zugriffe sollte die Einwilligung der Patientin / des Patienten ausreichen. Die *BFH* fragt, weshalb eine Gesundheitsfachperson informiert werden müsse, wenn es einen Remote-Zugriff für Support Zwecke gibt und ob es nicht eher Sinn mache, mindestens auch die Patientin / den Patienten zu informieren. Die Rolle Supporter sollte zudem in den Metadaten aufgenommen werden.

12. Aufhebung des elektronischen Patientendossiers (Art. 20 EPDV)

Die *OFAC* schreibt bezüglich der Ziffer 12.1.1, dass das elektronische Patientendossier nur im Falle eines Widerrufs der Einwilligung oder dem Tod gelöscht werden solle. Im Falle des Nichtgebrauchs seien nur die Dokumente zu löschen, jedoch nicht das elektronische Patientendossier, nicht die PID und auch nicht von der Patientin / dem Patienten eingegebene Daten, welche keiner Löschungsfrist gemäss Ziffer 10.1.2 unterliegen.

12.2 Bedingungen zur Aufhebung des elektronischen Patientendossiers (Abs. 1)

Die *K3* und der *VZK* schreiben, dass die Regelung gemäss Ziffer 12.2 bereits in der EPDV enthalten sei und deshalb hier weggelassen werden könne. Ähnlich beschreiben der Kanton *ZH* und der *ZAD* die Ziffer 12.2 als entbehrlich und fordern ebenfalls deren Streichung. 6 Kantone[155] wiederholen ihre Stellungnahme betreffend Artikel 20 EPDV und fordern die Streichung von Ziffer 12.2.1.2. *SBC* fragt bezüglich Ziffer 12.2.1.3, ob der Prozess auch ausgelöst werde, wenn die Patientin / der Patient ihre / seine Daten für die Forschung spendet oder sie / er diese den Erben übergibt. Ähnlich schreibt *economiesuisse*, dass die Daten von verstorbenen Patientinnen / Patienten exportiert werden können müssten, damit sie bspw. für die Forschung zur Verfügung gestellt werden können. Dies bedürfe allerdings der Einwilligung der Patientin / des Patienten gemäss Verfügung oder jene der Hinterbliebenen. Die *SGMI* macht geltend, dass eine Aufhebung im Todesfall unmittelbar nicht zulässig sei. Evtl. müsse aus medico-legalen Gründen auf die Daten zugegriffen werden können. Es wird vorgeschlagen, dass die Aufhebung erst nach einer Karenzfrist von z.B. 360 Tagen erfolgen dürfe.

12.3 Aufhebung des elektronischen Patientendossiers (Abs. 2)

Die *K3*, der *VZK*, der Kanton *ZH* und der *ZAD* wiederholen ihre Stellungnahmen von Ziffer 12.2 bezüglich Ziffer 12.3. Die *K3* und der *VZK* weisen zudem darauf hin, dass die Aufhebung des elektronischen

[155] FR, NE, GE, VS, VD, JU

Patientendossiers nicht nur in der Verantwortung der Stammgemeinschaften liegen könne, sondern Regelungen im Vertrauensraum des elektronischen Patientendossiers erfordere. 6 Kantone[156] schreiben, dass im Falle der Aufhebung des elektronischen Patientendossiers im Rahmen von Artikel 20 EPDV die Daten nicht sofort zu zerstören, aber auszublenden und unzugänglich zu machen seien. Die Löschung erfolge dann nach 10 Jahren. Ziffer 12.3 sei dementsprechend anzupassen und eine Ziffer mit dem Titel „Masquage du dossier électronique du patient" unter Ziffer 12.3 hinzuzufügen. Gemäss dem *USB* ist zu prüfen, ob die Aufhebung nicht erst nach einer Übergangsfrist erfolgen dürfe/solle. Zudem seien die Begriffe Aufhebung / Vernichtung / Löschung über alle Verordnungen hinweg zu klären bzw. zu erläutern. Der *VGIch* bezeichnet den Sinn und Zweck der Informationspflicht an alle Gemeinschaften gemäss Ziffer 12.3.1.4 als unklar. Falls die Informierung notwendig sei, solle evtl. die ZAS, allenfalls automatisiert, andere Gemeinschaften informieren. Weiter sei ein Widerruf grundsätzlich sofort gültig. Es stelle sich die Frage, wie die angemessen Frist gemäss Artikel 20 EPDV interpretiert werden soll. Die TOZ wiederhole den Begriff der Angemessenheit. Die TOZ soll technische und organisatorische Zertifizierungsvoraussetzungen enthalten und nicht die Verordnung interpretieren. Es sei ratsam eine Frist (z.B. einen Monat) in der EPDV vorzugeben. *SBC* fragt seinerseits, durch wen die Informierung aller Gemeinschaften und Stammgemeinschaften erfolge. Das *KSSG* stellt die Frage, wie eine solche Aufhebung in allen angeschlossenen Gemeinschaften realisiert werden solle und ist der Meinung, dass eine technische und somit automatisierte Information geschafft werden müsse. Es wird die Ausarbeitung eines entsprechenden IHE-Profiles vorgeschlagen.

12.4 Widerruf der Einwilligung zur Führung eines elektronischen Patientendossiers (Abs. 2 Bst. a)

6 Kantone[157] bemängeln, dass der Widerrufs-Prozess durch die Patientin / den Patienten selber mittels des Patientenportals nicht in Ziffer 12.4.1 beschrieben sei. Sie wünschen, dass dieser Prozess bei dieser Ziffer hinzugefügt wird. Die *Post* schreibt bezüglich Ziffer 12.4.1.2, dass der Widerruf auch elektronisch erfolgen könne und fragt, wie dann damit umzugehen sei. Sie beantragt, dass die Forderung angepasst wird. Zudem fragt sie zu Ziffer 12.4.2.1.2, ob eine Patientin / ein Patient für die Löschung ihres / seines elektronischen Patientendossiers persönlich vorsprechen müsse, wenn sie / er ihr / sein IDM nicht mehr nutzen könne. Auch hier solle die Forderung angepasst werden. Eine schriftliche Kündigung müsse genügen.

12.5 Schliessen bei Nichtgebrauch (Abs. 2 Bst. b)

6 Kantone[158] verweisen auf ihren Kommentar zu Artikel 20 EPDV und fordern die Streichung von Ziffer 12.5. *SBC* fragt, durch wen die Vorgabe gemäss Ziffer 12.5.1 zu detektieren sei. Der *VGIch* spricht sich für den folgenden Zusatz zu Ziffer 12.5.1.1 aus: „[…] Aufhebung darüber nachvollziehbar informiert wird".

3.2.3 Art. 3 Metadaten (Anhang 3)

Art. 3 Metadaten
Die Metadaten nach Artikel 9 Absatz 3 Buchstabe b EPDV sind in Anhang 3 festgelegt.

Artikel 3: 6 Kantone[159] fragen, was die Verbindung mit der von eHealth Suisse, in Zusammenarbeit mit den Kantonen, festgelegten Metadaten-Liste sei. Als Beispiel führen sie die Liste der Dokumente, klassifiziert nach den LOINC-Codes auf. Sie wünschen, dass die LOINC-Liste, welche bereits übersetzt sei, von den Kantonen seit mehreren Jahren verwendet werde und mit den internationalen Praktiken harmonisiert sei, wieder aufgenommen wird.

[156] FR, NE, GE, VS, VD, JU
[157] FR, NE, GE, VS, VD, JU
[158] FR, NE, GE, VS, VD, JU
[159] FR, NE, GE, VS, VD, JU

Anhang 3

1.1 Rolle des Autors: Die *BFH* ist der Meinung, dass mit 40999 „Andere“ zwar viel „erschlagen“ werden könne, trotzdem erscheine es wichtig zu überlegen, welche Rolle Administratoren, Supporter oder Personen spielen, die z.B. als Dienstleister ein Dossier für Bürgerinnen und Bürger in Zukunft vielleicht auch ausserhalb eines konkreten Behandlungspfades anlegen, damit diese ihre LifeStyle-Daten oder bereits ältere Dokumente hochladen können. *ChiroSuisse* weist darauf hin, dass bei dem nationalen Code 40003 die deutsche Bezeichnung falsch sei. Es werde folgende Formulierung beantragt: Chiropraktor (nicht „Chiropraktiker“). Der *SBK*, die *SWOR* und der *SVBG* bemängeln, dass Therapeutin / Therapeut (Nationaler Code 40011) als Überbegriff für verschiedene Berufe verwendet werde. Die Berufsbezeichnungen seien vollständig aufzuführen. Gemäss der *FMH* sei die deutsche Übersetzung für „Social Worker“ (Nationaler Code 40010) falsch. Sie fordern die Übernahme der korrekten Berufsbezeichnung „Sozialarbeiter FH“. Des Weiteren seien mit „Complementary therapist“ (Nationaler Code 40006) nicht ärztlich-komplementärmedizinisch Tätige gemeint. Es müsse die anerkannte Berufsbezeichnung in der Schweiz gemäss ODA-AM und ODA-AT verwendet werden. Der Kanton *BS* fragt, ob die „Case Managerin“ / der „Case Manager“ bei den „Social Worker“ (Nationaler Code 40010) enthalten sei. Aus den Metadaten heraus müsse ersichtlich sein, welcher Gesundheitseinrichtung die „Case Managerin / der „Case Manager“ angehört. Der Kanton *ZH* und *pharmaSuisse* sprechen sich dafür aus, die Rolle „Pharmacist“ (Nationaler Code 40001) analog Ziffer 1.2 Code 50045/50046 in „Retail pharmacist“ und „Hospital pharmacist“ aufzuteilen, da sich diese deutlich unterscheiden würden.

1.2 Medizinische Fachrichtung des Autors: Das *KSSG* weist darauf hin, dass die Fachrichtung Onkologie fehle, womit diese noch eingefügt werden müsse. Radioonkologie sei nicht dasselbe. Die *HÄ CH* und die *ÄTG* kritisieren, dass die Einteilung viel zu differenziert sei. So stünden alleine für Pflegende 6 verschiedene Auswahlmöglichkeiten offen. Sie fordern eine Vereinfachung. Die *SMCF* macht geltend, dass die Liste der medizinischen Fachrichtungen auf dem Anhang 1 der Medizinalberufeverordnung (MedBV) basieren solle und zudem die Berufsbezeichnung „Praktischer Arzt“ hinzugefügt werden sollte. *PharmaSuisse* macht darauf aufmerksam, dass der Begriff „Pharmacologist“ (Nationaler Code: 50040) korrekt übersetzt „Pharmakologe“ bedeute. Es gebe ärztliche und pharmazeutische Pharmakologen. Falls dieser Code ausschliesslich für Ärzte verwendet werden sollte, wird empfohlen, der englische Ausdruck in z.B. „Medical Pharmacologist“ abzuändern. Es seien ausserdem die aktuellen Bezeichnungen der nationalen Codes 50045 und 50046 in „Retail Pharmacist FPH“ („Apotheker FPH in Offizinpharmazie“) resp. „Hospital Pharmacist FPH“ („Apotheker FPH in Spitalpharmazie“) anzupassen. Des Weiteren wird empfohlen, die Begriffe „Clinical Pharmacist FPH“ („Apotheker FPH in Klinischer Pharmazie“) und „Pharmaceutical administrative assistant“ („Pharma-Betriebsassistentin“) zu ergänzen. Der Kanton *BS* schreibt, dass einige Ausdrücke (z.B. „Allergist“) im Englischen nicht gebräuchlich seien und schlagen die Prüfung der Anpassung der Benennung dieser Fachrichtungen vor. Weiter fehle die Spezialisierung der Labormedizin, weshalb geprüft werden solle, ob „specialist for laborytory medicine“ als Fachrichtung zu ergänzen sei. Des Weiteren stelle sich die Frage, ob bezüglich „specialized nurse“ (Nationaler Code 50065) die Ausbildungen nicht noch weiter spezifiziert werden sollten und die Spezialisierung des Pflegefachpersonals nicht als eigenständige Fachrichtung zu führen seien. Der *SBK*, die *SWOR* und der *SVBG* fordern, dass die medizinischen Fachrichtungen neutral zu formulieren seien und keine Kombinatorik aus Berufsbezeichnung und medizinischer Fachrichtung geführt werden solle (z.B. Rolle: Ärztin/Arzt, Dachrichtung: Gynäkologie). Zudem wünschen sie, dass die Berufsbezeichnungen der Pflege (Nationaler Code 50062 bis 50068) unter der Rolle aufgezählt werden.

1.3 Verfügbarkeitsstatus des Dokumentes: Die *BINT* und die *Integic* bemängeln, dass hinsichtlich des Dokumentlebenszyklus und Korrekturen im elektronischen Patientendossier keinerlei Angaben in den Dokumenten getätigt seien. Ausführungen hierzu wären wünschenswert. Der Kanton *ZH* wünscht die Ergänzung von den zusätzlichen Klassen „Patient Medication“ für die eDokumente der eMedikation und „Vaccination Information“ für die Daten des eImpfdossiers. Der Kanton *BS* weist bezüglich des Verfügbarkeitsstatus des Dokumentes darauf hin, dass der Ausdruck „deprecated“ äusserst ungewöhnlich und nicht verständlich sei. Das Gegenteil von „approved“ sei „denied“. Es solle geprüft werden, ob nicht ein

verständlicherer Begriff verwendet werden kann. Der *VGIch* schreibt, dass pro Dokument eine Versionierung sicherzustellen sei und zusätzlich von „gültigen" und „annullierten" Dokumenten gesprochen werde. Zudem könne ein Dokument gemäss den „Metadaten" einen Verfügbarkeitsstatus „genehmigt" und „abgelehnt" aufweisen. Der *VGIch* schlägt vor, dass die Terminologie zum besseren Verständnis geklärt und ggf. vereinheitlicht werden solle.

1.4 Dokumentenklasse: Das *KSSG* schreibt, dass anders als bisher publiziert, wieder Nationale Codes verwendet werden. Die Dokumentenklasse solle an einen internationalen Standard gebunden werden (ISO 13606). Das *LUKS* empfindet die Bezeichnungen der Differenzierungen als unklar (z.B. 70006 und 70010). Es wird ein Anwenderleitfaden ausserhalb des Ausführungsrechts gefordert. Die *BINT* und die *Integic* weisen darauf hin, dass die Zuordnung der möglichen Konstellationen/Intersektionen zwischen Dokumentenklasse/-typ erforderlich sei. Es solle eine Ergänzung / Umstrukturierung vorgenommen werden. Die *HÄ CH* und die *ÄTG* schreiben bezüglich Dokumentenklassen, dass die derzeit in Entwicklung befindlichen Dokumente / Austauschformate im Zusammenhang mit der eMedikation, eImpfung und eTOC in die Liste einfliessen müssen und laufend der Entwicklung angepasst werden. *PharmaSuisse* empfiehlt die Ergänzung der Klassen „Patient Medication" (Medikation des Patienten) für die eDokumente der eMedikation und „Vaccination Information" (Impfdaten) für die Daten des eImpfdossiers. Die *FMH* schreibt, dass die Klassen 70001 und 70002 zusammengelegt werden können in 70007/2 „Verlaufseintrag". Bei 70009 und 70013 sei zudem die Abgrenzung nicht klar. Evtl. könnten auch diese Klassen zusammengelegt werden in „Meldungen/Warnungen" Die *BFH* fragt, ob der Medikationsplan (60005) unter die Klasse 70012 falle. Hier wären ein paar Erläuterungen hilfreich, allenfalls auch eine jeweils aktualisierte Liste von im elektronischen Patientendossier-Biotop vorhandenen standardisierten CDA-Dokumenten und zur welcher Dokumentenklasse und Typ (Ziffer 1.12) diese zugeordnet sind.

1.5 Vertraulichkeitsstufe: Die *SQS* weist darauf hin, dass die Vertraulichkeitsstufe mit dem Code 30002 in Englisch und Deutsch gleich geschrieben werden müsse, was momentan nicht der Fall sei. Der Kanton *BS* macht betreffend der Vertraulichkeitsstufe 30005 darauf aufmerksam, dass „secret" auf Deutsch ein Geheimnis bedeute und schlägt zur Prüfung vor, ob der Begriff „protected data" nicht zutreffender wäre.

1.6 Format des Dokumentes: Für 7 Stellungnehmende[160] stellt sich die Frage, ob die Liste vollständig sei. Es könne kaum sein, dass das elektronische Patientendossier nur aus diesen 3 Dokumententypen bestehe. Sie fordern, 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. Des Weiteren wird gefordert, dass die Auflistung der Dokumententypen auch vom BAG weitergepflegt werden könne, ohne dass eine neue Verordnung notwendig werde. Die Austauschformate für den Medikationsplan oder den Austrittsbericht seien bereits geplant und müssten rasch in den Erlasstext aufgenommen werden. Die *IG eHealth* und die *Post* machen darauf aufmerksam, dass der Begriff in Französisch „Format du document" sich auf die Form des Dokumentes und nicht den Inhalt beziehe. Diese Bedeutung vom Format wurde insbesondere im Anhang 6 §3 (Indikatoren) und in der TOZ 2.2.1.3 verwendet. Sie beantragen, dass ein geeigneter Begriff (z.B. Austauschformat) verwendet werde und Begriffe definiert und konsistent über alle Texte benutzt werden. Der *HÄ CH* und die *ÄTG* fragen bezüglich des Formats der Dokumente, ob nicht auch noch die Dokumente zu eMedikation und eTOC hinein gehören würden. Die *SGMI* und das *LUKS* schlagen vor, weitere Dokumententypen (z.B. Laborwerte im Transplantationsprozess) aufzunehmen.

1.7 Typ der Gesundheitseinrichtung: Die *Medgate* bemängelt, dass die Zuordnung von Telemedizin-Dienstleistern unklar sei und fordert einen eigenen Code für telemedizinische Einrichtungen. *PharmaSuisse* empfiehlt den Code 20009 „Pharmacy" mit der deutschen Übersetzung „Öffentliche Apotheke" zu versehen. Gemäss dem Kanton *BS* mache das Wort „private" im Code 20004 „private home-based care" eine Aussage zur Finanzierungsform und sollte deshalb nicht an dieser Stelle stehen. Eine Umbenennung auf „home-based care" wird gewünscht. Des Weiteren wäre „nursing home" (Code 20008) auf Deutsch ein Pflegeheim. Es sei zu prüfen, ob „sozio-medizinische Institution" im Englischen

[160] IG eHealth, KSSG, medshare, Integic, HL7, IHE, BINT

nicht präziser wiedergegeben werden könne. *SCH* schlägt die Aufnahme von „Telemedizin“ als nationale OID vor. Die *FMH* macht folgende Anmerkungen: Code 20001: Systematische Auflistung der diagnostischen Institute oder Oberbegriff „diagnostische Institute“ verwenden; Code 20002: Übersetzung: „Notfallstation“; Code 20004: Bezeichnung: „Spitex“; Code 20010: zu präzisieren in ärztlich / nicht ärztlich; Code 20012: Übersetzung falsch.

1.8 Sprache des Dokumentes: Der *HÄ CH* und die *ÄTG* machen darauf aufmerksam, dass Hausarztpraxen immer wieder auch Dokumente aus den Heimatländern von Patientinnen / Patienten (z.B. Türkei) erhalten würden, weswegen zumindest eine Gruppe „other“ noch zu überlegen wäre. Die *HL7*, *IHE* und die *BINT* machen geltend, dass die Codes „de“, „fr“, „it“, „en“ (ohne –CH oder –US) ebenfalls zugelassen sein müssen. Ländererweiterungen seien wegzulassen oder zumindest diejenigen Codes ohne Ländererweiterung auch zu erlauben. Für die *IG eHealth* und die *Post* erscheint es wenig praktikabel, dass diese Liste als abschliessend formuliert sei. Sie fragen wie damit umgegangen werden solle, wenn eine Patientin / ein Patient ein Dokument in einer anderen Sprache hochladen möchte. Die Liste könne entweder als Beispiel oder als Minimalanforderungen definiert werden. Die nachfolgende Liste werde im Gesundheitswesen verwendet: Referenzierung zu OID 1.0.639.1[161]. Die *Post* fügt diesbezüglich an, dass alle ISO Sprachcodes erlaubt sein sollten.

1.9 MIME Typ des Dokumentes: 14 Stellungnehmende[162] weisen darauf hin, dass die Liste Doppelnennungen und damit redundante Daten enthalte, weswegen sie zu bereinigen sei. Gemäss der *HL7*, *IHE*, der *medshare* und der *Integic* müsse für „application/pdf“ zusätzlich festgehalten werden, dass PDF/A verwendet werden muss. Sie verweisen diesbezüglich auf die Vorgaben im Bundesarchiv[163] sowie ELGA[164] und schreiben, dass alle in ELGA-CDA-Dokumente eingebetteten PDF-Dateien dem Standard PDF/A-1a (gemäss „ISO 19005-1:2005 Level A conformance“) entsprechen müssen. Die *IG eHealth* und die *Post* bezeichnen die Liste von Dokumentenformaten als sehr restriktiv, zudem würden einige häufig benutzte Formate fehlen (z.B. PNG). Des Weiteren sei die Definition der Formate auch sehr unpräzise. TIFF sei unterstützt, es werde aber nicht definiert, welche Extension von TIFF unterstützt sein müsse. Sie beantragen, dass die Liste von Dokumentenformaten als Minimalanforderung formuliert werden sollte. Der Kanton *ZH* plädiert für eine Ergänzung der zulässigen Formate. Die *BFH* fragt, weshalb nur CDA Level 1 berücksichtig sei. Das *USB* erklärt in ihrer Bemerkung u.a. das Datenformat STL und spricht sich für dessen Aufnahme in die MIME-Tabelle als Dokumententyp aus.

1.10 Medizinische Fachrichtungen der in dem Dokument erfassten Daten: Das *KSSG* wiederholt ihre Stellungnahme aus Ziffer 1.2 „Medizinische Fachrichtung des Autors“. Die *ChiroSuisse* weist darauf hin, dass der englische Begriff von Code 10007 falsch sei und beantragt die Formulierung „Chiropractic“. *PharmaSuisse* und der Kanton *ZH* empfehlen, die Fachrichtungen „Pharmakotherapie (pharmacotherapy) und Patient Care (Betreuung chronisch kranker Patienten) zu ergänzen. Die *SGMI*, das *LUKS* und die *FMH* machen geltend, dass man durch die Kombination der medizinischen Fachrichtung und Typ des Dokumentes mehr Freiheitsgrade erhalten würde und die referentielle Integrität besser abgebildet wäre. Die Ziffern 1.10 und 1.12 seien in diesem Sinne zu überarbeiten.

1.11 Geschlecht der Patientin oder des Patienten: *PharmaSuisse* ist der Meinung, dass das Geschlecht für das Suchen und Finden eines Dokumentes nicht benötigt werde und deshalb nicht in den Metadaten angegeben werden sollte. Zudem bestehe die Gefahr einer missbräuchlichen Verwendung einer solchen Suchfunktion. Es wird dementsprechend die Streichung von Ziffer 1.11 vorgeschlagen.

1.12 Typ des Dokumentes: Die Kantone *GE*, *VS*, *VD*, *JU* und *FR* wiederholen ihre Stellungnahme von Artikel 3 EPDV-EDI. Die *BFH*, die *BINT* sowie die *Integic* wiederholen ihre Kommentare von Ziffer 1.4

[161] http://www.hl7.org/oid/index.cfm?Comp_OID=1.0.639.1
[162] BFH, HIN, HL7, IHE, medshare, Integic, K3, VZK, PharmaSuisse, ZH, SQS, LUKS, SGMI, FMH
[163] https://www.bar.admin.ch/bar/de/home/archivierung/ablieferung/digitale-unterlagen.html
[164] https://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/CDA/Implementierungsleitfaeden_2.06.1/HL7_Implementation_Guide_for_CDA_R2_-_Allgemeiner_Implementierungsleitfaden_fuer_ELGA_CDA_Dokumente_V2.06.1.pdf

und die *SGMI*, die *FMH* sowie das *LUKS* ihre Stellungnahmen von Ziffer 1.10. Das *KSSG* schreibt, dass anders als bisher publiziert wieder Nationale Codes verwendet werden. Die Dokumentenklasse solle an die internationalen LOINC-Codes gebunden werden. *PharmaSuisse* empfiehlt im Hinblick auf ihre Stellungnahme zu Artikel 4 / Anhang 4 die Ergänzung folgender Dokumententypen: eAbgabe-/Anwendungsdokument (Dispensation Record), Kommentar zur Medikation (eMedication comment) und Labordaten (Laboratory data). Die *Post* schreibt, dass gemäss Empfehlung von eHealth Suisse jeder Dokumenten-Typ genau einer Dokumentenklasse zugeordnet sein solle. Leider sei die Zuordnung jedoch offen (keine Vorgaben / Empfehlungen). Falls nun jede Gemeinschaft, oder sogar Gesundheitsfachperson, eine eigene Zuordnung machen würde, entstünden Inkonsistenzen beim Austausch innerhalb oder zwischen den Gemeinschaften. Die *Post* beantragt deshalb Vorgaben, wie die Dokumententypen genau einer Dokumentenklasse zugeordnet werden müssen. Die *STSAG* bemängelt, dass bei Code 60037 „Progress Note“ nicht zur Übersetzung „Kurve“ passe und schlägt „Verlaufsbericht Intensivstation“ vor. Der Kanton *BS* schlägt vor, bei Code 60006 den englischen Begriff auf „Electronic prescription“ umzubenennen. Zudem weist *BS* darauf hin, dass bei Code 60027 der englische Ausdruck falsch sei. Histologie heisse „histology“ und nicht jede Histologie stamme aus einer Biopsie. Die Zytologie erscheine nirgends und müsse noch eingefügt werden.

3.2.4 Art. 4 Austauschformate (Anhang 4)

Art. 4 Austauschformate
Die Austauschformate nach Artikel 9 Absatz 3 Buchstabe c EPDV sind in Anhang 4 festgelegt.

Artikel 4: Die *BRH* schreiben, dass die medizinischen Austauschformate jene Daten enthalten würden, um welche es im elektronischen Patientendossier im eigentlichen gehe und im Zentrum des medizinischen Datenaustauschprozesses stehen. Diese sollen gemäss Erläuterung im Rahmen von Stakeholderprozessen erarbeitet werden und seien nicht Teil des Ausführungsrechts. Die Definition von Austauschformaten (zumindest Minimal Data Set) mit Eingang in das EPDV-EDI wird vorgeschlagen. Die *SGMI* stellt fest, dass die Austauschformate noch nicht vorliegen und gemäss BAG in Stakeholderprozessen erarbeitet werden sollen. Es wird ein möglichst früher Einbezug der Stakeholder gefordert, damit ein effizienter, effektiver Prozess mit nachhaltigem Ergebnis stattfinden könne. *PharmaSuisse* bedauert, dass der Anhang 4 noch nicht existiert und macht darauf aufmerksam, dass Austauschformate dem Austausch von Informationen zwischen den Gesundheitsfachpersonen dienen. Je mehr Informationen einem Behandelnden zur Verfügung stehen, desto besser könne er die Behandlung einer Patientin / eines Patienten optimieren, was die Patientensicherheit erhöhe. Es wird sehr begrüsst, dass ausschliesslich die Patientin / der Patient über die Steuerung der Zugriffsrechte definiere, welche Dokumente von einem Behandelnden eingesehen werden können und dass somit grundsätzlich sämtliche Informationen von allen Behandelnden jeder Berufsgruppe zur Verfügung stünden. Ebenfalls begrüsst wird, dass Anhang 4 „im Rahmen von Stakeholderprozessen“ erarbeitet werde und mittels zukünftiger Revisionen in das Ausführungsrecht aufgenommen werden solle. Der Anhang 4 sei rasch möglichst zu erstellen und solle den Beratungen der IPAG entsprechen. Die *HL7* und *IHE* schreiben, dass nur 4 Formate festgelegt seien und dass Informationsobjekte hier einen entscheidenden Einfluss hätten. Analog *Bleuer* weisen sie darauf hin, dass bei den Ergebnissen der bildgebenden Diagnostik auf absehbare Zeit noch folgender Use Case üblich bleiben werde: Bilder und Befundberichte etc. erhält die Patientin / der Patient auf einer CD/DVD zusammen mit einem Viewer. Solche Viewer seien z.T. proprietär; selbst wenn die Daten im DICOM Format vorliegen, seien sie nicht immer mit allen Viewern kompatibel. Es müsse also die Möglichkeit bestehen, CD/DVD mit Bildern, Befundberichten etc. zusammen mit den jeweiligen Viewern im elektronischen Patientendossier vorzuhalten; z.B. mittels ZIP-Format. ZIP ist auch zu unterstützen, weil in DICOM zulässig (Details s. DICOM PS3.12). Der *VLSS* bemängelt, dass die EPDV, aber auch die EPDV-EDI, vernehmlasst werden, bevor man sich über die Austauschformate geeinigt habe. Diese seien vielmehr gar nicht Gegenstand der Vorlage, so dass man mit einer Zustimmung zu den erwähnten Verordnungen dieses Kernstück aus ärztlicher Sicht sozusagen „im Sack“ kaufen würde. Ihnen sei das „Interprofessionale Fallbeispiel“ aus der Vernehmlassung, welche die FMH dazu intern durchführe, zwar durchaus bekannt. Die Ausführlichkeit der beabsichtigten Austauschformate erstaune sie aber sehr. Anstatt sich auf das Notwendige und Nützliche zu beschränken, sollen gemäss dieser Vorgabe im Rahmen des elektronischen Patientendossiers zusätzlich zum ärztlichen

Teil umfangreiche Krankengeschichten für die Bereiche Probleme, Anamnese, Behandlungen und Verlauf durch sämtliche an der Behandlungskette beteiligten Gesundheitsfachpersonen geführt werden. Dies sei weder zielführend noch realistisch. Der Blick aufs Wesentliche gehe verloren und es würden riesige Datenfriedhöfe entstehen, die dann vom BAG trotz gesetzlichem Auftrag nicht ausgewertet werden können, weil zu wenige Patientinnen / Patienten ein elektronisches Patientendossier wollten.

3.2.5 Art. 5 Integrationsprofil (Anhang 5)

Art. 5	Integrationsprofile
Anhang 5 legt in Anwendung von Artikel 9 Absatz 3 Buchstabe d und e EPDV fest:	
a.	die Integrationsprofile;
b.	die nationalen Anpassungen der Integrationsprofile;
c.	die nationalen Integrationsprofile.

Artikel 5: Der Kanton *NE* schliesst sich dem Kommentar vom Kanton *FR* zum Artikel 1 EPDV-EDI an dieser Stelle an. Die *H+* begrüsst, dass das EDI auf international anerkannte, auch in der Schweiz etablierte technische Standards zurückgreife. Wichtig sei, dass den Gemeinschaften und Stammgemeinschaften aufgrund ihrer juristischen Ausgestaltung nicht verwehrt bleibe, auf vorhandenen Datenaustausch-Plattformen des eGovernment mitzuwirken.

Anhang 5a

Die Kantone *GE*, *VS*, *VD*, *JU* und *FR* schreiben, dass sie nicht die Kompetenz hätten, um diesen Anhang zu kommentieren und dieser von IHE Suisse validiert werden müsse. Die *OFAC* vertraut IHE Suisse bezüglich Standardisierung und Dokumentation der Integrationsprofile. Ähnlich verlässt sich das *KSSG* auf die Stellungnahme von IHE Suisse und HL7. Der Kanton *SG* verweist auf die Prüfung durch IHE Suisse und HL7 und fügt an, dass Integrationsprofile fehlen würden, welche das Löschen über die Gemeinschaften hinweg definieren. Gemäss dem *LUKS* sei wichtig, dass das Ausführungsrecht des EPDG mit der technischen Entwicklung Schritt halte. Insbesondere seien die kommenden Entwicklungen des HL7 Standard FIHR zu berücksichtigen und zuzulassen. Für die weitere Beurteilung und Überarbeitung sei IHE Suisse und HL7 einzubeziehen. Die *IG eHealth* und die *POST* sind der Meinung, dass diese Vorschrift so keinen Sinn mache. Die definierten IHE-Profile seien teilweise für den Einsatz innerhalb einer Affinity Domain und teilweise für den Einsatz "Cross Community" vorgesehen. Der Gesetzgeber habe festgelegt, dass das Gesetz den Bereich zwischen den Gemeinschaften regelt. Darum mache es keinen Sinn Profile zu definieren, welche ausschliesslich für den Einsatz innerhalb von Affinity Domains gemacht wurden. Zudem sei auch nicht klar, wie diese Liste von Profilen zu interpretieren sei. 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 *IG eHealth* und die *Post* schlagen vor, dass die Formulierung zwischen MUSS (MUST) und SOLL (SHOULD) Profilen unterscheiden sollte. Die *Integic* schreibt bezüglich folgendes: „1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption“: RESTful- ATNA sei ein neues Supplement for Trial Implementation und solle aufgenommen werden (Add RESTful Query to ATNA - Published 2015-08-07)[165]. Neben der vorgeschlagenen Lösung über National Extention sei auch eine Lösung mit IHE RESTful-ATNA verfügbar. Die *SGMI* und *SBC* weisen darauf hin, dass Lieferanten von IT-Komponenten diese registrieren lassen sollten (Homologation). Weiter sollte die Registrierung von IT-Systemen komplett von der Gemeinschaftszertifizierung getrennt werden. Dies würde ermöglichen, dass signifikante Einsparungen bei der Zertifizierung der einzelnen Gemeinschaften erzielt würden, da die technischen Komponenten schon registriert werden, es gäbe eine klare Verantwortungsverteilung zwischen den Lieferanten von IT-Komponenten und der Gemeinschaft, es entstünde ein offener Markt für die technischen Komponenten, es würde eine Vereinfachung des Beschaffungsprozesses für die Gemeinschaft erfolgen und es gäbe eine Unterstützung für „best of breed“-Infrastruktur, die

[165] http://wiki.ihe.net/index.php/ATNA_Repository_RESTful_Access
http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

kein geschlossenes Ecosystem eines Lieferanten sein werde, entsprechend werde eine Stimulation der Industrie erwartet. Die *SGMI* und *SBC* schlagen vor, dass die Zertifizierung einer Gemeinschaft, die registrierte Komponenten einsetzt, die Registrierungsprozedur der technischen Infrastruktur nicht wiederholen müsse, sondern nur die organisationalen Prozesse und Datenschutz-Massnahmen zertifizieren lassen. Weiter schreibt die *SGMI*, dass Anträge von IHE Suisse unterstützt seien. *HIN* bezeichnet die Übersicht und die tabellarische Kurzbeschreibung als sehr hilfreich und die *medshare* begrüsst den Weg über die Integrationsprofile sehr. Die *FMH* beantragt wiederum die Streichung, da sie gegen die Regelung auf Verordnungsebene sei.

Anhang 5b

1.1 Definitions of terms

Die *Post* und die *IG eHealth* schreiben bezüglich Ziffer 1.1 folgendes:

1.1.1: - Die Formulierung „may" widerspreche der Dokumentationspflicht für Gesundheitsfachpersonen und folgende Formulierung sei besser: „Healthcare professionals must save this data".
- Betreffend des Textteils „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.
- Betreffend des Textteils "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.
- Betreffend Figure 1: Why is this called "Unique person identification"? Clarify terminology

1.1.3: - The term "base community" was introduced (and translated 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? Clarify terminology.

1.1.4: - CCO is the only institution which is allowed to correlate the Social Security Number (AVN13) with the electronic patient dossier-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 habe eine direkte Auswirkung auf die Umsetzung.
- Betreffend des Textteils „the gateways may correlate": Why is it not must? Some transactions like patient discovery mandate the use of the electronic patient dossier-PID as the only identifier. Antrag: "may" durch "must" ersetzen. Werde das nicht geändert, dann könne es zu Kompatibilitätsproblemen kommen.

HIN schreibt bezüglich des Textteils „Primary Systems may correlate their local patient identifier with the MPI-PID", dass mit dem Begriff "Primary Systems" vermutlich das Primärsystem in Gesundheitsbetrieben gemeint sei. Falls diese Annahme korrekt ist: In 2.11.1 Anhang 2 (TOZ) stehe u.a., dass die PID nicht direkt und dauerhaft mit Dokumenten der Patientinnen und Patienten verknüpft werde. Diese Aussage der TOZ und die Aussagen hier erscheinen widersprüchlich und müssen aufgelöst werden. Des Weiteren sei der Begriff „HIS" nicht erklärt. Wahrscheinlich heisse dies „Hospital Information System". Der Begriff sei in das Glossar aufzunehmen.

1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption

Die *BINT* und die *medshare* machen darauf aufmerksam, dass neben der vorgeschlagenen Lösung über National Extention auch eine Lösung mit IHE RESTful-ATNA verfügbar sei. RESTful-ATNA sei ein neues Supplement for Trial Implementation und solle aufgenommen werden. Zudem wird in diesem

Zusammenhang eine Wiki-Link[166] angegeben. Während die *BINT* zudem auf ein Dokument bezüglich RESTful-ATNA vom 07.08.2015[167] verweist, gibt die m*edshare* ein Dokument mit Datum 27.05.2016[168] an. Die *Post* schreibt zudem folgendes: 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 be replaced with a two tiered approach of ATNA logs for legal purposes and some higher abstraction level of event logging for end users.

1.4.2: Die *Integic* weist darauf hin, dass Actor Document Consumer nicht abfragend in Richtung Audit Record Repository agiere, sondern nur schreibend im Sinne der Record Audit Event (ITI-20) Transaction. Ein Audit Record Repository sei keine XDS-b fähige Actor Komponente. Der Workflow in der beschriebenen Form sei nicht IHE-konform. Eine Präzisierung oder Auflösung dieser Ausführungen werde dringend empfohlen, da eine ITI-18 und eine folgende ITI-43 von Doc Consumer an ARR nicht den genannten IHE-Profilen entsprechen würden. Die *HL7* und *IHE* schreiben folgendes: Registry Stored Query [ITI-18] transaction that uses the parameters described in chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10. Retrieve Document Set [ITI-43] transaction performed against an Audit Record Repository using a document UUID received by a previously executed by a Registry Stored Query mentioned before. Sie fordern die Streichung. Die *Post* und *IG eHealth* geben folgendes betreffend Ziffer 1.4.2 zu Protokoll:
- „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.
- 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 patient will hardly be able to interpret the contents of the ATNA audit log. 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.
Die *IG eHealth* fügt zudem folgenden Punkt an: 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. Die *Integic* macht betreffend Ziffer 1.4.2.2 darauf aufmerksam, dass nur der Actor Secure Application angeführt sei. Vor allem Gemeinschaften bzw. Zusammenschlüssen Registry und Repository seien definitiv als Secure Node auszuführen bzw. der Actor sei hier zu ergänzen. Die *HL7* und *IHE* wünschen folgende Umformulierung des Textteiles „These actors […] ATNA Audit Repositories" von Ziffer 1.4.2.3: „If the parameter $XDSDocumentEntryTypeCode contains the value 60049 (Audit trail), the responding gateway must return an UUID for a subsequent retrieval of an On Demand Document returning the audit messages matched by the filter parameters in the query of the corresponding document UUID in the 1.4.4.1 ATNA Audit Message Format. See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10". Des Weiteren schreiben sie bezüglich Ziffer 1.4.2.4.1, dass nicht verordnet werden müsse, wie die gemeinschaftsinterne Auditabfrage realisiert werde. So könne z.B. auch IHE RESTful ATNA eingesetzt werden. Für Ziffer 1.4.2.5 verlangen sie zudem die Streichung des ersten, des dritten und des vierten der 4 im Text aufgeführten Bullet Points.

1.4.3: Die *Integic* weist darauf hin, dass ITI-57 nur ConfidentialityCode ändern dürfe, was betreffend Versionierung Fragen hervorrufe. Eine Stornierung eines Dokuments im elektronischen Patientendossier, das im Zuge der Abbildung von Dokumentenlebenszyklen (siehe ITI-41 RPLC) in Document Registry verzeichnet ist müsse erlaubt sein. Die *IG eHealth* und die *Post* beantragen bezüglich Ziffer

[166] http://wiki.ihe.net/index.php/ATNA_Repository_RESTful_Access
[167] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf
[168] http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA_Rev2.0_PC_ 2016-05-27.pdf

1.4.3.2 folgendes: Instead of UUID this should read documentUniqueId. Zu Ziffer 1.4.3.1.2 schreiben sie zudem folgendes: „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.

1.4.4: Die *Integic* empfiehlt betreffend AuditMessage/ActiveParticipant, nicht nur die UserID, sondern einen lesbaren Namen der durchführenden Person als 1.1 mandatory Element einzuführen, um die Protokollierung für die Patientin / den Patienten nachvollziehbarer zu gestalten. *HIN* stellt fest, dass GLN bei Ziffer 1.4.4.1.1 als „MUSS“ definiert sei. In der Verordnung (Artikel 24 EPDV) sei aber erwähnt, dass sie übermittelt werden "kann", also optional ist. Dies scheine widersprüchlich zu sein. Es gebe Fälle, bei denen die GLN noch undefiniert sei. Es wird vorgeschlagen, die GLN überall als „MUSS“ zu haben. Dies bewirke, dass Praxen erst eine GLN lösen müssen, bevor sie einer Gemeinschaft beitreten können. Die *Post* und die *IG eHealth* schreiben folgendes zu Ziffer 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 pre-defined format. Zu Ziffer 1.4.4.1.1 geben sie zudem folgendes zu bedenken: Which time zone is used in a timestamps string representation is completely irrelevant as long as the time zone is included in the string representation so downstream processes interpret it correctly. Antrag: remove the Swiss national extension.

1.5 Requirements on PIXv3 for Patient Identity Feed

Die *Post* und die *IG eHealth* schreiben betreffend OtherIDs folgendes: From the documents of EPDV storing the electronic patient dossier-PID in the MPI is a MUST requirement. Why is it a MAY requirement here? Correct the requirement.

1.7 Requirements on PDQv3 Profile for Patient Demographics Query

Betreffend Ziffer 1.7.2.1.1 ist folgendes für die *Post* und die *IG eHealth* unklar: 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 Requirements on XCPD Profile for Cross-Community Patient Discovery

Die *Post* und die *IG eHealth* zeigen in ihrer Stellungnahme ein Case auf und fragen, wie dieser zu lösen sei. Zudem fordern sie folgendes: An example for patient matching across communities should be provided. Bezüglich Ziffer 1.8.2 schreiben sie zudem folgendes: 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”.

1.9 Requirements on HPD Profile for Replication

HIN wiederholt ihre Stellungnahme von Ziffer 1.4.4.1.1 bezüglich den Ziffern 1.9.5.1.1 und 1.9.5.1.2.

Anhang 5c

1 Introduction

Das *KSSG* fragt betreffend dem Einsatz von XDS-I, ob der DICOM WADO Service ebenfalls Bestandteil der Zertifizierung sei. Dieser wäre Bestandteil der Primärsysteme wenn im XDS Repository nur das KOF registriert werde. Weiter interessiert, ob die Patientenzugangsportale einen entsprechenden DICOM Viewer, der mit WADO (Akteur Imaging Document Consumer) umgehen kann, unterstützen müssen und ob dies zertifizierungsrelevant sei. Der ganze Bereich XDS-I für den Austausch von Bilddaten sei in den TOZ nicht berücksichtigt worden, weswegen die EPDV und die TOZ gemäss der Anforderung aus IHE XDS-I zu überprüfen seien. Die *Post* und die *IG eHealth* schreiben bezüglich des Textteiles "It has been specified for the Document Registries to act as Policy Enforcing Service Providers in terms of a XACML PEP" folgendes: 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.
Sie sind zudem der Meinung, dass diese Art der Vorgaben es sehr schwierig machen, dass verschiedene Anbieter eigene Lösungen umsetzen können. Die *IG eHealth* beantragt folgendes: Do not specify HOW something must be implemented. Specify the desired result instead.

2 Volume 1 – Integration Profiles

Die *IG eHealth* und die *Post* schreiben bezüglich Ziffer 2.2 folgendes:
- 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".

- Subject: The custodian attribute has to be present in addition to the GLN/ electronic patient dossier-ID. Authorization decisions can only be made for GLN/ electronic patient dossier-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 electronic patient dossier-ID. Antrag: Be more specific about which attributes co-exist on a subject.

- Attribute Statement: organization & organization-id: Carrying organization text and ID attributes for patients makes little sense. Resource-id = electronic patient dossier-PID: This assumes that there will never be any cross-patient use cases. This appears to be not very future proof. Antrag: Do not require org text and org ID attributes for patients. Drop electronic patient dossier-PID as resource attribute.

Für die *Integic* scheint eine Gültigkeitsdauer von 10 Minuten für die Praxis als zu kurz gewählt. Die Wartezeit sei auf 30 bis 60 Minuten zu verlängern. Betreffend Ziffer 2.3.2 weisen die *Post* und die *IG eHealth* auf folgendes hin: XACML 3.0 was published in Jan. 2013. is there a reason to use an outdated version? It should keep up with current standards.

3 Volume 2 – Transactions

Die *IG eHealth* und die *Post* schreiben bezüglich Ziffer 3.1.10 folgendes: „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 habe direkte Auswirkungen auf die Implementierung und die Performance. Antrag: Drop the attribute. Zudem geben sie folgende Stellungnahme für Ziffer 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 habe ebenfalls direkte Auswirkungen auf die Implementierung und die Performance. Antrag: Add trigger event "RetrieveDocumentSetRequest". Die *Integic* macht darauf be-

züglich Ziffer 3.1.6.1 darauf aufmerksam, dass „ADR due to XDS Register Document Set-b“ der Abschnitt 3.1.6.2 sein sollte. Die *IG eHealth* und die *Post* schreiben bezüglich der Ziffer 3.1.6.1 folgendes: The approach of “bulk querying the PDP” does not scale for 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. The PEP must be able to operate on the registry response stream in order to scale. The bulk request approach also does not scale if other document attributes become part of the access decision. The number of combinations to bulk-query for grows exponentially with the number of attributes and their values. The paragraph should be seen as an implementation example for small result sets. But as the size of the result is unknown, unless fully un-marshaled into memory, it is rather useless from an implementation perspective. Another example based on response stream filtering should be added. Die *medshare* weist bezüglich Ziffer 3.3 darauf hin, dass das technische Austauschformat zur Policy, welche mit CH:PPQ ausgetauscht werde, fehle und zu spezifizieren sei. Bezüglich Ziffer 3.3.9 schlägt *Integic* vor, dass „ACMLPolicyQuery Response“ auf „XACMLPolicyQuery Response“ korrigiert wird.

3.2.6 Art. 6 Evaluation (Anhang 6)

Art. 6 Evaluation
Gemeinschaften und Stammgemeinschaften müssen dem BAG für die Evaluation nach Artikel 21 Absatz 2 EPDV die Daten nach Anhang 6 zur Verfügung stellen.

Artikel 6: 6 Stellungnehmende[169] wünschen die Ergänzung dieses Artikels um die Vorgabe, dass die Gemeinschaften die entsprechenden Daten dem BAG nur in anonymisierter Form liefern dürfen. Aus den in Anhang 6 aufgeführten Daten ergebe sich, dass dies für die geplanten Auswertungen ausreicht. Es sei folgender, neuer Absatz 2 einzufügen: „Die Gemeinschaften und Stammgemeinschaften sind verpflichtet, die Daten vor der Weiterleitung an das BAG zu anonymisieren oder anonymisieren zu lassen“. Gemäss den Kantonen *GE*, *VS*, *VD* und *JU* seien die folgenden, angeforderten Indikatoren zu präzisieren: - betrachtete Zeitdauer, - global oder pro Patientin / Patient, - die Frequenz, - der Durchschnitt, - der Median, - absolute Zahlen, etc. Die Errichtung dieser Indikatoren werde für die Gemeinschaften Kosten verursachen, welche vom Bund abgedeckt werden sollten. Der Text sei mit der Angabe des Finanzrahmens zu vervollständigen. Die *HL7*, *IHE* und die *medshare* fordern die Festlegung von Periodizität und Fristen. *HIN* spricht sich dafür aus, dass die Reportinganforderungen praktikabel bleiben sollen. Insbesondere sollte das Reporting auf Anfrage und nicht per se erfolgen. Artikel 6 sei demnach folgendermassen zu ergänzen: „Gemeinschaften und Stammgemeinschaften müssen dem BAG auf Anfrage nach […]“. Die *SGMI* macht darauf aufmerksam, dass die Daten resp. Kennzahlen bezüglich Grunddaten, Zugriffrechten, Dateien, Nutzung und Datenschutz auf ein absolutes Minimum zu beschränken seien und nicht zum Zweck der Kontrolle der Leistungserbringer missbraucht werden sollen. *Santésuisse* schreibt, dass im Hinblick auf die Evaluation der Zweck- und Zielerreichung von Gesetz und Verordnung gemäss EPDG (Art.1 Abs. 3) in den Erläuterungen jeglicher Hinweis auf die Konkretisierung der durchzuführenden Evaluation fehle. Die im Anhang 6 aufgeführten Kennzahlen vermögen den Anforderungen einer Evaluation des elektronischen Patientendossiers hinsichtlich Verbesserung der Behandlungsqualität, der Behandlungsprozesse, der Patientensicherheit, etc. ihrer Ansicht nach in keiner Weise zu genügen.

Anhang 6

1. Grunddaten: Die *OFAC* schreibt, dass die durch die Artikel 39 und 49a des Bundesgesetzes über die Krankenversicherung (KVG) betroffenen Spitäler und anderen Einrichtungen ihr Anschlussdatum, wahrscheinlich dem BAG, offenlegen müssen. Diese Information habe keine Relevanz in einem Evaluationsindikator. *HIN* weist darauf hin, dass die Kombination von Alter, Geschlecht und Wohnort in Einzelfällen nicht ausreichend anonym sein könne. Es müsse die Anonymität der Patientinnen / Patienten

[169] KDSBSON, DSBAG, privatim, FR, BE, ZG

gewährleistet sein. Sie schlagen die folgende Formulierung bei der zweiten Kennzahl vor: „[…] nach Alter, Geschlecht und Wohnort, wobei ein noch zu definierendes Clustering bei Gruppen kleiner als 7 anzuwenden ist“. Zudem wird eine Erklärung gewünscht, was genau mit Wohnort gemeint sei. Die *Post* macht geltend, dass die Kennzahl, welche die Aufschlüsselung nach Alter, Geschlecht und Wohnort beinhalte, in den Kennzahlen von Ziffer 1 und Ziffer 2 aufgeführt sei. Dies sei zu korrigieren resp. die Kennzahl an einem Ort zu löschen.

2. Zugriffsrechte: *HIN* und die *Post* wiederholen ihre Stellungnahme von Ziffer 1. Die *SGMI* und die *FMH* sind der Ansicht, dass die Zugriffsrechte für Evaluation irrelevant und unverhältnismässig seien. Die *SGMI* fordert eine Überarbeitung. Gemäss der *STSAG* sind die Anzahl und Art der Dateien pro Vertraulichkeitsstufe auf Stufe EDI als irrelevant einzustufen und entsprechen nicht einer sinnvollen Kennzahlenevaluation. Die Aussagekraft ist gering und der daraus abgeleitete Handlungsspielraum fraglich. Vor einer unnötigen Sammlung von Daten sollte abgesehen werden. Dasselbe gelte für die Anzahl ausgeschlossener Gesundheitsfachpersonen. Diese Kennzahl sei dementsprechend zu streichen. Das *LUKS* stellt fest, dass die Zugriffsrechte in der Entscheidungshoheit der Patientinnen / Patienten seien. In welchem Umfang sie diese einschränken oder erweitern sei für die Evaluation nicht relevant. Ob und wer vom Notfallzugriff Gebrauch gemacht hat, könne der die Patientin / der Patient im Portal des elektronischen Patientendossiers einsehen. Ziffer 2 sei zu überarbeiten. Das *KSSG* macht darauf aufmerksam, dass die Erhebung solcher Kennzahlen relativ komplex erscheine, da mit dem Punkt 4.14.1.9 der TOZ die Speicherung von patientenbezogenen Daten in ATNA und Logfiles, etc. verboten werde.

3. Dateien: Gemäss dem *LUKS* gebe die Anzahl der eingestellten Dokumente keine Aussage zum Nutzen des elektronischen Patientendossiers. Die *SGMI* und *FMH* bezeichnen die Anzahl Dateien zur Evaluation als irrelevant und unverhältnismässig und auch die *STSAG* attestiert der Anzahl eingestellter Dateien, aufgeschlüsselt nach Format Irrelevanz. Das *LUKS*, die *SGMI*, die *FMH* und die *STSAG* fordern die Streichung dieser Kennzahl. Die *Post* weist darauf hin, dass der Begriff „Format“ für einen anderen Zweck benutzt werde und gemäss Anhang 3, §1.6, der Begriff „Mime Type“ benutzt werden müsste.

4. Nutzung: Die *FMH*, die *SGMI* und das *LUKS* sind der Meinung, dass diese Daten für die Evaluation nicht relevant seien und sehen in der Erhebung dieser eher die Absicht einer Kontrolle, weshalb die Kennzahl zu streichen sei. Das *KSSG* weist darauf hin, dass die Kennzahlen betreffend der Nutzung nur teilweise geliefert werden können, da einige Attribute nicht Bestandteil der Metadaten seien. *HIN* schreibt, dass hier die Begriffe "Dateiklasse" und "Datei-Art" eingeführt werden. Es werde angenommen, dass sich "Dateiklasse" auf "Dokumentenklasse" (Kap. 1.4 im Anhang 3) und "Datei-Art" auf "MIME Typ des Dokuments" (Kap. 1.9 im Anhang 3) beziehe. Falls das falsch sei, wäre eine Klarstellung im Text gewünscht. Die *Post* bemängelt, dass bei den Kennzahlen die Begriffe "Dateiklasse" und "Datei-Art" nicht definiert seien und beantragt, dass entweder eine Definition nachzuliefern sei, oder aber die vermutlich korrekten Begriffe "Dokumentenklasse" und "Dokumenten Typ" aus Anhang 3 verwendet werden. Betreffend der Statistik über Löschung von Daten schreibt die *Post*, dass es keine Möglichkeit für die Patientin / den Patienten gebe, ein Dokument zu löschen. Sie / Er könne die Geheimstufe ändern. Die Indikatoren seien zu löschen. Des Weiteren schreibt die *Post* bezüglich der letzten Kennzahl unter Ziffer 4, dass eine Zahl pro Patientin / Patient definiert werde. Sie fragt, welche Daten darzustellen seien (PID, Name, Vorname, …) oder was anonymisiert werde. Dies sei zu präzisieren oder zu löschen. Gemäss der *STSAG* müsse die Anzahl der Gesundheitsfachpersonen nicht erhoben werden. Der Nutzen sei gering und bei grösseren Institutionen die Aussagekraft irrelevant. Eine Erhebung durch die Stammgemeinschaft reiche zudem aus. Zudem haben Dateiklassen und Dateiart wenig Aussagekraft, weshalb Kennzahlen in diesem Zusammenhang zu streichen seien. Des Weiteren sei die Zugriffsauflistung im zeitlichen Verlauf aufwändig und habe wenig Aussagekraft. Hier reiche eine Erhebung durch die Stammgemeinschaft ebenfalls aus. Dasselbe gelte für die Patientenzugriffe (sowohl zeitlicher Verlauf als auch Dateiklassen und –art).

5. Datenschutz: Der Kanton *SG* fragt, was als Reklamation gelte und spricht sich für eine genaue Definition aus.

3.2.7 Art. 7 Mindestanforderungen an das Personal (Anhang 7)

Art. 7	Mindestanforderungen an das Personal
Die Mindestanforderungen an die Qualifikation des Personals nach Artikel 27 Absatz 4 EPDV, welches Zertifizierungen durchführt, sind in Anhang 7 festgelegt.	

Artikel 7: Die *SGMI* macht geltend, dass die Anforderungen an die Zertifizierung Personal sehr hoch seien. Die *SQS* wiederholt ihre Stellungnahme von Artikel 27 Absatz 4 EPDV und fordert die ersatzlose Streichung von Artikel 7.

Anhang 7

Bezüglich Ziffer 1.1.1 schreibt die *SQS*, dass die 'Technischen und Organisatorischen Voraussetzungen', welche Gemeinschaften und Stammgemeinschaften zu erfüllen haben, primär keine Inhalte aufweisen, welche spezifische Kenntnisse in Medizininformatik bedingen würden, um eine regelkonforme Überprüfung im Rahmen der Zertifizierung zu garantieren. Des Weiteren sollen gemäss dem erläuternden Bericht zum EPDG die Anforderungen an die Kompetenz einer Zertifizierungsstelle in Anwendung von international breit abgestützten Grundsätzen und Verfahren festgelegt werden. Falls die Zertifizierung nach VDSZ als Zertifizierungsnorm gewählt werde, seien die Bedingungen für das Personal der Zertifizierungsstellen bestimmt, indem die VDSZ im Anhang die Mindestanforderungen an die Qualifikation des Personals der Zertifizierungsstellen regelt. Ebenso werden in ISO/IEC 27006 (falls nach ISO 27001 zertifiziert wird) oder ISO 17021 die Kompetenzen des Personals geregelt. Im Rahmen von Ziffer 1.1.5 fügt die *SQS* zudem an, dass die ISO/IEC 27006 nur dann relevant sei, wenn nach ISO/IEC 27001 zertifiziert werden müsse. Auch in diesem Fall seien die Anforderungen an die Qualifikation des Personals der Zertifizierungsstelle durch die Akkreditierung gegeben. Die Ziffern 1.1.1 und 1.1.5 seien ersatzlos zu streichen. *HIN* plädiert bezüglich den Ziffern 1.1.1, 1.1.2, 1.1.3, 2.1.1, 2.1.2 und 2.1.3, dass 5 Jahre Berufserfahrung (anstatt 2) zu bevorzugen sei, falls eine spezifische Ausbildung fehlt. 2 Jahre seien ausreichend in Kombination mit einer zusätzlichen Ausbildung. Zusätzlich schreibt *HIN*, dass eine konkret geforderte Anzahl Berufsjahre in den entsprechenden Sparten (Medizininformatik, Datenschutz) mit 2 Jahren Berufserfahrung oder 1 Jahr Ausbildung als an der unteren Grenze liegend erscheine. Für derart wichtige Tätigkeiten wie Zertifizierungen in sensiblen Bereichen wie Patientendaten erscheinen Personen mit mehr Erfahrung notwendig. *HIN* begrüsst aber, dass die ID-Provider wie auch Gemeinschaften zertifiziert werden sollen. Für die *SGMI*, die *FMH* und das *LUKS* sind die Anforderungen an die Zertifizierungsstellen zu hoch angesetzt, was den Wettbewerb gering und die Kosten hochtreiben werde. Trotz diesen überaus anspruchsvollen Anforderungen dürfte im täglichen Betrieb keine Verbesserung der Datensicherheit erreicht werden. Diese hänge erfahrungsgemäss mehr vom Nutzerverhalten, als von den technischen Schutzmassnahmen ab. *Lovis* schreibt, dass die Zuverlässigkeit und Verantwortung gewährleistet werden müsse. Die *OFAC* weist bezüglich Ziffer 1.1.2 darauf hin, dass eine juristische Inkohärenz bestehe. Die Gemeinschaften, die als kantonale Stelle durch die Kanton verwaltet werden, würden unter das kantonale Datenschutzrecht fallen. Es bestünden grosse Unterschiede: Kein Kanton sehe in seinem eigenen Datenschutzrecht die Einführung eines Datenschutzmanagementsystems vor, die mit der DSG- und EDÖB-Doktrin über Selbstregulierung in Widerspruch stehe. Kein Kanton sehe in seinem eigenen Datenschutzrecht zudem ein Zertifizierungsverfahrensprozess vor. Weiter schreibt die *OFAC*, dass sie nicht direkt von diesem Anhang betroffen sei und möchte, dass die auf die Zertifizierungsorganisationen anwendbaren Anforderungen nicht von denen, die bereits in Kraft und von der Schweizerischen Akkreditierungsstelle (SAS) verwaltet sind, abweichen.

3.2.8 Art. 8 Schutz der Identifikationsmittel (Anhang 8)

Art. 8	Schutz der Identifikationsmittel
Die Vorgaben für den Schutz der Identifikationsmittel nach Artikel 30 Absatz 2 EPDV sind in Anhang 8 festgelegt.	

Artikel 8: Die *IG eHealth* schreibt, dass dem Anspruch der Patientinnen / Patienten an Einfachheit und

Klarheit hohe Priorität eingeräumt werden müsse, da eine umständliche Anwendung eine grosse Zugangshürde zum elektronischen Patientendossier darstelle. Daher gelte es im Rahmen der nötigen Sicherheitsanforderungen auch die Praktikabilität mittels einfachen Grundregeln/Voreinstellungen sicherzustellen. Anhang 8 müsse überarbeitet werden. Für den Erfolg des elektronischen Patientendossiers sei es wichtig, sowohl sichere als auch bequeme IDM anzubieten. Erfahrungsgemäss würden Smart Cards auf wenig Akzeptanz stossen und es gäbe grosse betriebliche Herausforderungen in Bezug auf Kompatibilität mit einer vorhandenen IT-Infrastruktur wie auch auf die Ausgabeprozesse. Systeme wie mTAN oder Verfahren, die biometrische oder verhaltensbasierte Mechanismen nutzen, seien de facto ausgeschlossen. Es sei sicherzustellen, dass IDM mit genügendem, kantonal akzeptiertem Schutzniveau in Spitälern auch für den Zugriff auf das elektronische Patientendossier verwendet werden dürfen. Es dürfe nicht sein, dass hier zusätzliche Investitionen notwendig sind. Wo rechtlich zulässig sei zudem zu vermeiden, dass doppelte Identifikationen (IDM für spitalinterne Zugriffe und separates IDM für Zugriffe auf das elektronische Patientendossier) eingesetzt werden müssen.

Anhang 8

1.2 TOE Overview

Die *OFAC* macht darauf aufmerksam, dass der Begriff „EPDG“ in „FLEHR“ übersetzt wurde, während bei der „EPDV“ auf die englische Übersetzung verzichtet wurde. Entweder man halte sich an die strikte Regeln, die spezifische EPDG-Terminologie ins Englische zu übersetzen, oder man übersetzt alle Texte in die verschiedenen Landessprachen. Ausserdem seien die Logos und Übersetzungen des Bundes, des EDI und des BAG über das gesamte Dokument hinweg nicht einheitlich. Sowohl Logos, wie auch Übersetzungen müssen homogen sein und idealerweise in die Sprache des Dokumentes übersetzt werden. Die *Post* macht bezüglich Ziffer 1.2.1 darauf aufmerksam, dass die TOE Definition weder biometrische noch verhaltensbasierte Verfahren der Authentisierung erlaube. Ohne diese Anpassung werde mTAN nicht möglich sein. Sie beantragt, dass die Definitionen aus ISO 29115, Kapitel 3.3, übernommen werden, anstatt eine "Device" Definition einzuführen. Weiter weist sie bezüglich Ziffer 1.2.2 darauf hin, dass der Begriff „identification means“ falsch verwendet werde. „Authentication means“ seien Mittel um den Authentisierungsprozess abzuwickeln, während „idenfication means“ Mittel seien, um den Identifikationsprozess abzuwickeln. Dies sei zu korrigieren. Weiter deute der Begriff „holder of the token“ darauf hin, dass Verfahren, die ohne Token auskommen, de facto verboten seien. Der Begriff „Token“ soll durch den Begriff „authentication factor“ aus ISO 29115 ersetzt werden. Des Weiteren deute die Beschreibung des TOE darauf hin, dass nur IdP basierte Verfahren überhaupt zugelassen seien. Es stelle sich die Frage, was mit Verfahren passiere, die keinen IdP benötigen. Das TOE solle so formuliert werden, dass das Authentisierungsverfahren und das Verfahren via IdP beschrieben seien. Schliesslich werde noch ein Begriff „Context“ eingeführt. Dieser habe im Zusammenhang mit der Authentisierung nichts zu suchen. Authentisierung soll verifizieren, ob die behauptete Identität korrekt ist. Kontext sei eine Frage der Autorisierung. Sollte der Identity Provider diesen Kontext benötigen, um ein geeignetes Verfahren zur Authentisierung auszuwählen, dann sei das „Out of Scope“ für dieses Dokument. Die Referenzen zum Kontext seien daher zu löschen oder als optional zu markieren. *SCH* macht bezüglich Ziffer 1.2.2 geltend, dass die Ausführungen über den Workflow für die Authentisierung sehr detailliert seien. Dabei werde jedoch nur der IdP-Initated Approach beschrieben. Es sollte den Applikationsherstellern für das elektronische Patientendossier überlassen werden, welchen Workflow, IdP- oder RP-initiated Approach sie für die Authentisierung bevorzugen. Zudem sollten die Protokolle zwischen Relying Party und IdP sowie die Authentisierungsverfahren vom Markt geregelt werden. Im Weiteren wäre die Benutzerführung einfacher, wenn die Benutzerin / der Benutzer zuerst auf das Portal des elektronischen Patientendossiers navigiert werde und sich danach einloggen könne. Dies entspreche den erlernten Erwartungen von vielen Benutzern. Dadurch werde auch die Akzeptanz des elektronischen Patientendossiers erhöht. *SCH* beantragt, dass der IdP-initiated Workflow für die Authentisierung weggelassen wird. Es sollten nur die Voraussetzungen und Resultate der Authentisierung festgehalten werden, nicht jedoch vorgeschrieben werden, mit welchen Schritten dies erreicht werden müsse. Zudem schreiben *SCH* folgendes als Vorschlag: Electronic identification means comprises one or more token that are secured by a device. Each token may hold a credential, that is used by the IdP to authenticate

the user's identity based on possession and control of the corresponding token. An IdP-initiated or SP-initiated approach may be used.

1.5 Assets

Die *Post* weist bezüglich Table 1 darauf hin, dass die Beschreibungen so geschrieben seien, dass ausschliesslich smart card basierte Verfahren möglich sind. Wenn das nicht geändert werde, dann seien mTAN oder andere Mittel ohne smart card nicht möglich. Es wird gefordert, dass die Definitionen aus ISO 29115, Kapitel 3.3, übernommen werden. Zudem schreibt die *Post* folgendes bezüglich Ziffer 1.5:
- Public keys by definition are public and they need to protection. Es sei eigentlich klar, was gemeint ist, aber die Formulierung sei falsch. Antrag: Term to be used here is "private keys".

- The expectation in the example of "identification data" is not tenable. Using a combination of attributes to uniquely identify a user seems like a bad choice. Please note that GLN is an extremely dangerous example: GLN is unique for a person. Unfortunately in the health care system of Switzerland we have quite a number of health care providers that work in different organizations that may or may not be members of different communities. Depending on the context of the person, this person may have different users (at least one in each community). Das sei eine reine Frage der Terminologie. Antrag: use proper terminology. use good examples.

- Table 1: Assertion Data: SAML assertions are the only supported standard to transport claims about the authenticated identity. This is geared towards SOAP web services and not practical for HTTP based services. Falls dies nicht geändert werde entstünden mit der Integration von neuen FHIR IHE-Profilen und Mobilgeräten Probleme. Antrag: Support for HTTP based services should be included.

- There are several references in the document to the purpose of login to a web portal. This precludes purposes like authentication of web services, REST interfaces or mobile applications. Antrag: The purpose should be formulated openly. Further references should be avoided.

- Table 1: The following description is not an "English" sentence; "The IdP stores enough information about the authentication means of the user to validate the user". The IdP must ensure that the information stored about the authentication means of the user cannot be used to recover the authentication means itself. Antrag: change the formulation.

1.6 External Entities and Subjects

Die *Post* schreibt folgendes bezüglich Table 2 in Ziffer 1.6: - The term "identification token" has not been used before. The term identification means of identification token should not be used. The purpose of this token is to be used in the authentication process and it should be called authentication means. The term means is more generic than token since a means just implies that it can be used for the purpose instead of token, which implies a physical presence.

- We are missing the HelpDesk. This role also requires privileged access to be able to support end users. The terms trusted and privileged should be aligned.

- IdP: This abbreviation is wrongly explained. Die *Post* führt in ihrer Stellungnahme die Wikipedia-Erläuterung von IdP auf.

Die *Post* weist darauf hin, dass die aufgeführten Punkte eine reine Frage der Terminologie seien. Sie beantragt für alle beschriebenen Elemente folgendes: Use properly defined terms that avoid confusion.

3 Security Problem Definition

Die *Post* schreibt bezüglich Table 3 folgendes: CredentialHandling: The wording is geared towards smart card use. Wenn das nicht geändert werde, dann sei mTAN nicht möglich. Sie beantragt, dass die Definitionen aus ISO 29115, Kapitel 3.3, übernommen werden. *SCH* weist bezüglich CredentialHandling darauf hin, dass im Fall, in welchem die Benutzerin / der Benutzer ihre / seine Credentials selbständig revozieren kann, keine Kommunikation mit dem Service Desk des IdPs notwendig sei. Der letzte Satz in Table 3 unter CredentialHandling sei folgendermassen am Schluss des letzten Satzes zu ergänzen:

„[…] appropriate channels or that the claimant is able to revoke/reset his device/token through appropriate means". Weiter wünscht *SCH* im Rahmen von Ziffer 3.2 folgende Ergänzungen zur Policy P.Assertion: „SAMLID-Token has to comply with the specification given in section 6.3 or 6.4. The IdP information processing system shall contain a component to generate unique reference identifiers. A time restricted SAMLID-Token issued […]". Bezüglich P.TrustedCommunityEndpoint sei zudem folgendes anzufügen: "[…] as defined in section 6.3 or 6.4".

4 Security Objectives

Die *Post* schreibt bezüglich O.Confidentiality in der Tabelle von Ziffer 4.1 folgendes: Please note that all references to public keys in the user data conflict with this requirement. Public keys are made for dissemination. Das sei eine reine Frage der Terminologie. Antrag: modify the definition of user data. Weiter gibt sie bezüglich O.Authentication folgendes zu Protokoll: The explanation in the second paragraph should be aligned with ISO 29115. Das sei relevant für Akzeptierung von mTAN. Antrag: use the term "authentication factor". Weiter schreibt die Post unter Ziffer 4.2 bezüglich OE.User Security Awareness: This paragraph contains references to smart card registration processes. Wenn das nicht geändert werde, dann sei mTAN nicht möglich. Es wird beantragt, dass die Definitionen aus ISO 29115, Kapitel 3.3, übernommen werden. *HIN* weist bezüglich Ziffer 4.3.1 darauf hin, dass die Spalte „OE. SecureAreas and Equipment" mit keiner Zeile verknüpft sei. Gleiches gelte für die Zeile „A.Physical". Dies sei zu korrigieren resp. ergänzen.

5 Security Requirements

Die Post schreibt bezüglich Ziffer 5.2.12, FCS_COP.1(1), folgendes: Elliptic Curve keys are way smaller than RSA/DH/EG keys with comparable security[170]. Requiring an elliptic curve keys to be 2k in size makes no sense. Wenn das nicht geändert wird, dann werde die Sicherheit stehen bleiben. Mit den Referenzen entwickle sich das automatisch weiter. Es wird beantragt, dass Algorithmen nicht definiert werden, sondern die Empfehlungen des BSI oder des NIST referenziert werden. Weiter fügt die Post folgendes an: The referenced standard FIPS PUB 180-3 was superseded by FIPS PUB 180-4 in March 2012. Sie verweist an dieser Stelle auf die aktuellen Standards[171].

6 Appendix

Die *OFAC* schreibt bezüglich SAML in Ziffer 6.4, dass diese technische Restriktion nicht akzeptabel sei. SAML sei weder universal, noch unvergänglich. Der Betrieb der IDP und der Identifikationstoken müsse in Bezug auf die grundsätzlichen Anforderungen beschrieben werden und nicht zu technisch und einschränkend. *SCH* macht darauf aufmerksam, dass im vorliegenden Dokument ausschliesslich das SAML-Protokoll für die Authentisierung erwähnt werde. Es würden weitere etablierte Protokolle wie OpenID Connect basierend auf OAuth 2.0 existieren. Die Interoperabilität der IDM müsse sich auf die Formate der Personenidentifizierungsdaten beschränken. Die Protokolle zwischen Relying Party und IdP und die Authentisierungsverfahren sollten jedoch vom Markt her geregelt werden. Es wird beantragt, dass zusätzlich zur „SAML Specification" auch eine „OpenID Connect/ OAuth 2.0 Specification" erstellt werden. Zudem sollten die Verordnungen/Anhänge so gestaltet werden, dass weitere Protokolle hinzugefügt werden können. Folgender Vorschlag ist zudem in ihrer Stellungnahme enthalten: 6.5 OpenID Connect/OATH 2.0 Specification; Note: The specification will be drafted during or subsequently to appraisal.

[170] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Key_sizes
[171] http://csrc.nist.gov/publications/PubsFIPS.html

4. Anhänge

4.1 Liste der Stellungnehmenden

Die Liste umfasst sämtliche Anhörungsteilnehmende des Ausführungsrechts zum EPDG gemäss Tabelle 1.

Abkürzung	Kantone
AG	Staatskanzlei des Kantons Aargau Chancellerie d'Etat du canton d'Argovie Cancelleria dello Stato del Cantone di Argovia
AI	Ratskanzlei des Kantons Appenzell Innerrhoden Chancellerie d'Etat du canton d'Appenzell Rhodes-Intérieures Cancelleria dello Stato del Cantone di Appenzello Interno
AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden Chancellerie d'Etat du canton d'Appenzell Rhodes-Extérieures Cancelleria dello Stato del Cantone di Appenzello Esterno
BE	Staatskanzlei des Kantons Bern Chancellerie d'Etat du canton de Berne Cancelleria dello Stato del Cantone di Berna
BL	Landeskanzlei des Kantons Basel-Landschaft Chancellerie d'Etat du canton de Bâle-Campagne Cancelleria dello Stato del Cantone di Basilea Campagna
BS	Staatskanzlei des Kantons Basel-Stadt Chancellerie d'Etat du canton de Bâle-Ville Cancelleria dello Stato del Cantone di Basilea Città
FR	Staatskanzlei des Kantons Freiburg Chancellerie d'Etat du canton de Fribourg Cancelleria dello Stato del Cantone di Friburgo
GE	Staatskanzlei des Kantons Genf Chancellerie d'Etat du canton de Genève Cancelleria dello Stato del Cantone di Ginevra
GL	Regierungskanzlei des Kantons Glarus Chancellerie d'Etat du canton de Glaris Cancelleria dello Stato del Cantone di Glarona
GR	Standeskanzlei des Kantons Graubünden Chancellerie d'Etat du canton des Grisons Cancelleria dello Stato del Cantone dei Grigioni
JU	Staatskanzlei des Kantons Jura Chancellerie d'Etat du canton du Jura Cancelleria dello Stato del Cantone del Giura
LU	Staatskanzlei des Kantons Luzern Chancellerie d'Etat du canton de Lucerne Cancelleria dello Stato del Cantone di Lucerna
NE	Staatskanzlei des Kantons Neuenburg Chancellerie d'Etat du canton de Neuchâtel Cancelleria dello Stato del Cantone di Neuchâtel
NW	Staatskanzlei des Kantons Nidwalden Chancellerie d'Etat du canton de Nidwald Cancelleria dello Stato del Cantone di Nidvaldo

OW	Staatskanzlei des Kantons Obwalden Chancellerie d'Etat du canton d'Obwald Cancelleria dello Stato del Cantone di Obvaldo
SG	Staatskanzlei des Kantons St. Gallen Chancellerie d'Etat du canton de St-Gall Cancelleria dello Stato del Cantone di San Gallo
SH	Staatskanzlei des Kantons Schaffhausen Chancellerie d'Etat du canton de Schaffhouse Cancelleria dello Stato del Cantone di Sciaffusa
SO	Staatskanzlei des Kantons Solothurn Chancellerie d'Etat du canton de Soleure Cancelleria dello Stato del Cantone di Soletta
SZ	Staatskanzlei des Kantons Schwyz Chancellerie d'Etat du canton de Schwyz Cancelleria dello Stato del Cantone di Svitto
TG	Staatskanzlei des Kantons Thurgau Chancellerie d'Etat du canton de Thurgovie Cancelleria dello Stato del Cantone di Turgovia
TI	Staatskanzlei des Kantons Tessin Chancellerie d'Etat du canton du Tessin Cancelleria dello Stato del Cantone Ticino
UR	Standeskanzlei des Kantons Uri Chancellerie d'Etat du canton d'Uri Cancelleria dello Stato del Cantone di Uri
VD	Staatskanzlei des Kantons Waadt Chancellerie d'Etat du canton de Vaud Cancelleria dello Stato del Cantone di Vaud
VS	Staatskanzlei des Kantons Wallis Chancellerie d'Etat du canton du Valais Cancelleria dello Stato del Cantone del Vallese
ZG	Staatskanzlei des Kantons Zug Chancellerie d'Etat du canton de Zoug Cancelleria dello Stato del Cantone di Zugo
ZH	Staatskanzlei des Kantons Zürich Chancellerie d'Etat du canton de Zurich Cancelleria dello Stato del Cantone di Zurigo
Abkürzung	**Parteien**
FDP PLR PLR	FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali
SPS PSS PSS	Sozialdemokratische Partei der Schweiz Parti socialiste suisse Partito socialista svizzero
SVP UDC UDC	Schweizerische Volkspartei Union démocratique du Centre Unione democratica di Centro
Abkürzung	**Gesamtschweizerische Dachverbände der Wirtschaft**

economiesuisse	Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation
SGB	Schweizerischer Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)
SGV	Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e dei mestieri (USAM)
Abkürzung	**Übrige Organisationen**
CCC	Chaos Computer Club Schweiz
ChiroSuisse	Schweizerischen Chiropraktoren-Gesellschaft ChiroSuisse (SCG) Association suisse des chiropraticiens ChiroSuisse (ASC) Associazione svizzera dei chiropratici ChiroSuisse (ASC)
curafutura	Die innovativen Krankenversicherer Les assureurs-maladie innovants Gli assicuratori-malattia innovativi
CURAVIVA	Verband Heime und Institutionen Schweiz Association des homes et institutions sociales suisses Associazione degli istituti sociali e di cura svizzeri
FMH	Verbindung der Schweizer Ärztinnen und Ärzte (FMH) Fédération des médecins suisses Federazione dei medici svizzeri
FRC	Fédération romande des consommateurs (frc)
GELIKO	Schweizerische Gesundheitsligen-Konferenz Conférence nationale suisse les ligues de la santé Conferenza nazionale svizzera delle leghe per la salute
GDK CDS CDS	Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und Gesundheitsdirektoren (GDK) Conférence suisse des directrices et directeurs cantonaux de la santé (CDS) Conferenza svizzera delle direttrici e dei direttori cantonali della sanità (CDS)
H+	H+ Die Spitäler der Schweiz H+ Les Hôpitaux de Suisse H+ Gli Ospedali Svizzeri
HIN	Health Info Net AG
HL7	HL7 Benutzergruppe Schweiz
IG eHealth	Verein IG eHealth
IHE	IHE Suisse
ISSS	Information Security Society Switzerland
HÄ CH	Hausärzte Schweiz – Berufsverband der Haus- und Kinderärzte Médecins de famille Suisse – Association des médecins de famille et de l'enfance Suisse Medici di famiglia Svizzera – Associazione dei medici di famiglia e dell'infanzia Svizzera
OFAC	Berufsgenossenschaft der Schweizer Apotheker La cooperative professionelle des pharmaciens suisses La cooperativa professionale del farmacisti svizzeri

pharmaSuisse	Schweizerischer Apothekerverband Société suisse des pharmaciens Società svizzera dei farmacisti
PH CH	Public Health Schweiz Santé publique Suisse Salute pubblica Svizzera
Physioswiss	Schweizerischer Physiotherapie-Verband Association suisse de physiothérapie Associazione svizzera di fisioterapia
PKS	Privatkliniken Schweiz Cliniques privées suisses Cliniche private svizzere
privatim	privatim, Die schweizerischen Datenschutzbeauftragten privatim, Les préposé(e)s suisses à la protection des données privatim, Gli incaricati svizzeri della protezione dei dati
santésuisse	Verband der Schweizer Krankenversicherer Les assureurs-maladie suisses
SBK	Schweizerischer Berufsverband der Pflegefachfrauen und Pflegefachmänner (SBK) Association suisse des infirmières et infirmiers (ASI) Associazione svizzera delle infermiere e degli infermieri (ASI)
SGMI	Schweizerische Gesellschaft für Medizinische Informatik Société Suisse d'Informatique Medicale Società Svizzera d'Informatica Medica
Spitex	Spitex Verband Schweiz Association suisse des services d'aide et de soins à domicile Associazione svizzera dei servizi di assistenza e cura a domicilio
SPO	Stiftung SPO Patientenschutz (SPO) Fondation Organisation suisse des patients (OSP) Fondazione Organizzazione svizzera dei pazienti (OSP)
Stiftung refdata	Stiftung refdata Fondation refdata Fondazione refdata
SUVA	Schweizerische Unfallversicherungsanstalt (Suva) Caisse nationale suisse d'assurance en cas d'accidents Istituto nazionale svizzero di assicurazione contro gli infortuni
SVBG	Schweizerischer Verband der Berufsorganisationen im Gesundheitswesen (SVBG) Fédération suisse des associations professionnelles du domaine de la santé (FSAS) Federazione Svizzera delle Associazioni professionali Sanitari (FSAS)
SVV	Schweizerischer Versicherungsverband (SVV) Association suisse d'assurances (ASA) Associazione svizzera d'assicurazioni (ASA)
VGIch	Vereinigung Gesundheitsinformatik Schweiz
Abkürzung	**Nicht begrüsste Organisationen und Privatpersonen**
ahdis	ahdis gmbh
AHE	Altersheimverein Eigenamt
ALM	Alterszentrum Moosmatt
APP	Alters- und Pflegeheim Pfauen
ASG	Alterszentrum Schiffländi Gränichen
ASPS	Association Spitex privée Suisse
ÄTG	Ärztegesellschaft Thurgau

AZB	Alterszentrum Blumenheim
AZK	Alterszentrum Sunnmatte
AZSH	Alterszentrum Suhrhard AG
BEKAG	Ärztegesellschaft des Kantons Bern Société des médecins du canton de Berne (SMCB) Società dei medici del Cantone di Berna (SMCB)
Bethesda	Bethesda Alterszentren AG
BFG	Bündnis Freiheitliches Gesundheitswesen Entente Système de santé libéral
BFH	Berner Fachhochschule – Institute for Medical Informatics / Spitalzentrum Biel
BINT	BINT GmbH
Bleuer	Juerg P. Bleuer
BRH	Berner Reha Zentrum AG Heiligenschwendi
BüAeV	Bündner Ärzteverein BüAeV
DSBAG	Beauftragte für Öffentlichkeit und Datenschutz des Kantons Aargau
DSF	Datenschutz-Forum Schweiz
EHS	Verein eHealth Südost
FAAG	Asana Gruppe AG, Altersresidenz Falkenstein
FER	Fédération des entreprises romandes
GAeSO	Gesellschaft der Ärztinnen und Ärzte des Kantons Solothurn
GS1	GS1 Schweiz
HospizAG	Hospiz Aargau
ICTS	ICT Switzerland
Insel	Inselspital Universitätsspital Bern Hôpital universitaire de l'Ile, Berne Inselspital Ospedale universitario di Berna
Insos	Nationaler Branchenverband der Institutionen für Menschen mit Behinderung Association de branche nationale des institutions pour personnes avec handicap
Integic	Integic AG
K3	Konferenz Kantonale Krankenhausverbände
KAeG SG	Ärztegesellschaft des Kantons St. Gallen
KBAG	Klinik Barmelweid AG
KDSBSON	Datenschutzbeauftragter der Kantone Schwyz, Ob- und Nidwalden
KFSAG	Klinik für Schlafmedizin AG
KKA	Konferenz der kantonalen Ärztegesellschaften (KKA) Conférence des sociétés cantonales de médecine (CCM) Conferenza delle società mediche cantonali (CMC)
KMUF	KMU-Forum
KSOW	Kantonsspital Obwalden
KSSG	Kantonsspital St.Gallen
LEUG	Asana Gruppe AG, Spital Leuggern
Lovis	Christian Lovis
LUKS	Luzerner Kantonsspital
Medgate	Medgate AG
medshare	medshare GmbH
MENZ	Asana Gruppe AG, Spital Menziken
Moeri	Thomas Moeri
PINK	Schweizerische Schwulenorganisation PINK CROSS

Post	Post CH AG Poste CH SA Posta CH SA
PSV	Pflegeheim Sennhof AG
RCA	RehaClinic AG
RPB	Regionales Pflegezentrum Baden AG
RZPB	Reusspark Zentrum für Pflege und Betreuung
SBC	Serge Bignens Consulting
SBV	Schweizerischer Blinden- und Sehbehindertenverband Fédération Suisse des aveugle et malvoyants
SCH	Swisscom Health
SDG	Schweizerische Diabetesgesellschaft (SDG) Association suisse du diabète (ASD) Associazione svizzera per il diabete (ASD)
senesuisse	Verband wirtschaftlich unabhängiger Alters- und Pflegeeinrichtungen Association d'établissements économiquement indépendants pour personnes âgées
SMAG	Salina Medizin AG
SMCF	Société de Médecine du Canton de Fribourg
SQS	Schweizerische Vereinigung für Qualitäts- und Management Systeme (SQS) Association suisse pour systèmes de qualité et de management (SQS) Associazione svizzera per sistemi di qualità e di Management (SQS)
SteHAG	Verein der Stammgemeinschaft des Kanton Aargau
STSAG	Spital STS AG
SWICO	SWICO
SW!SS REHA	Vereinigung der Rehabilitationskliniken der Schweiz
SWOR	Swiss Orthoptics
SZW	Seniorenzentrum Wasserflue
Tessaris	Tessaris Integrated Security AG
USB	Universitätsspital Basel
VAKA	Verband Aargauische Spitäler, Kliniken und Pflegeinstitutionen
VDPS	Vereinigung der Direktoren der Psychiatrischen Kliniken und Dienste der Schweiz Association des directeurs de cliniques et hôpitaux psychiatriques en Suisse
VKZS	Vereinigung der Kantonszahnärzte und Kantonszahnärztinnen der Schweiz (VKZS) Association des médecins dentistes cantonaux de Suisse (AMDCS) Associazione dei medici dentisti cantonali della Svizzera (AMDCS)
VLSS	Verein der Leitenden Spitalärztinnen und -ärzte der Schweiz (VLSS) Association des médecins dirigeants d'hôpitaux de Suisse (AMDHS) Associazione medici dirigenti ospedalieri svizzeri (AMDOS)
VZK	Verband Zürcher Krankenhäuser
ZAD	Verein Trägerschaft ZAD

4.2 Weitere Abkürzungen und Begriffe

Abkürzung	Titel
AHVN13	Die 13-stellige AHV-Nummer
ATP	Attributeprovider
BAG OFSP UFSP	Bundesamt für Gesundheit Office fédéral de la santé publique Ufficio federale della sanità pubblica
(D)DoS-Angriffe	(Distributed) Denial-of-Service-Angriffe
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDI DFI DFI	Eidgenössisches Departement des Innern Département fédéral de l'intérieur Dipartimento federale dell'interno
GLN	Global Location Number
HPD	Health Provider Directory
IDM	Identifikationsmittel
IDP	Identifikationsprovider
IHE	Integrating the Healthcare Enterprise
IPAG EPD	Interprofessionelle Arbeitsgruppe Elektronisches Patientendossier
ISMS	Informationssicherheits-Managementsystem
KIS	Klinikinformationssystem
LOINC	Logical Observation Identifiers Names and Codes
MedReg	Register über die universitären Medizinalberufe
MPI	Master Patient Index
PID	Patientenidentifikationsnummer
PSP	Personensicherheitsprüfung
SaaS	Software as a Service
SIEM	Security Information and Event Management System
STL	Standard Transformation Language
STS	Secure Token Service
TOZ	Technische & organisatorische Zertifizierungsvoraussetzungen
WAF	Web-Application-Firewall
WZW	wirksam, zweckmässig und wirtschaftlich
XUA	Cross-Enterprise User Authentication
ZAS	Zentrale Ausgleichsstelle

4.3 Organisationen mit identischer Stellungnahme wie der Verband Aargauische Spitäler, Kliniken und Pflegeinstitutionen (VAKA)

An sämtlichen Stellen dieses Berichtes, an denen die nachfolgenden Organisationen nicht explizit aufgeführt sind, entsprechen deren Stellungnahmen derjenigen der VAKA	
Abkürzung	**Name**
AHE	Altersheimverein Eigenamt
ALM	Alterszentrum Moosmatt
APP	Alters- und Pflegeheim Pfauen
ASG	Alterszentrum Schiffländi Gränichen
AZB	Alterszentrum Blumenheim
AZK	Alterszentrum Sunnmatte
AZSH	Alterszentrum Suhrhard AG
Bethesda	Bethesda Alterszentren AG
FAAG	Asana Gruppe AG, Altersresidenz Falkenstein
HospizAG	Hospiz Aargau
KBAG	Klinik Barmelweid AG
KFSAG	Klinik für Schlafmedizin AG
LEUG	Asana Gruppe AG, Spital Leuggern
MENZ	Asana Gruppe AG, Spital Menziken
PSV	Pflegeheim Sennhof AG
RCA	RehaClinic AG
RPB	Regionales Pflegezentrum Baden AG
RZPB	Reusspark Zentrum für Pflege und Betreuung
SMAG	Salina Medizin AG
SteHAG	Verein der Stammgemeinschaft des Kanton Aargau
SZW	Seniorenzentrum Wasserflue