Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

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

Stellungnahme von

Name / Kanton / Firma / Organisation	: [Datenschutzbeauftragter Kanton Basel-Stadt]
Abkürzung der Firma / Organisation	:
Adresse, Ort	:
Kontaktperson	:
Telefon	:
E-Mail	:
Datum	:

Hinweise

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

1 Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG

Allgemeine Bemerkungen zu den Erlasstexten

Allgemeine Bemerkungen zu den Erläuterungen

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

Allgemeine Bemerkungen

Dieser Erlass ist aus datenschutzrechtlicher Sicht nicht von Bedeutung. Es wird daher auf eine Stellungnahme verzichtet.

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag

Bemerkungen zu den Erläuterungen

Seite / Artikel	Kommentar	Änderungsantrag

3 BR: Verordnung über das elektronische Patientendossier EPDV

Allgemeine Bemerkungen

Die EPDV erscheint sorgfältig ausgearbeitet. Sie berücksichtigt den Datenschutz je nach Themenbereich unterschiedlich zufriedenstellend. Die nachfolgenden Ausführungen fokussieren sich daher primär auf jene Bereiche, bei denen Anpassungsbedarf besteht.
Nachfolgend finden sich Anmerkungen zu drei Themenbereichen, die sich in der EPDV nicht geregelt finden:

Hilfspersonen: Es finden sich weder in der EPDV noch in den Erläuterungen Regelungen bzw. klärende Hinweise zu den Hilfspersonen. In den Diskussionen im Vorfeld der Gesetzgebungsprozesse waren diese jedoch wiederholt Thema. Dabei wurde festgestellt, dass es sich dabei um kein einfaches Thema handelt. Wir möchten darauf aufmerksam machen, dass die Regelung für Hilfspersonen, wie sie nun in den Erläuterungen zur EPDV (S. 15 f.) umschrieben ist, aus Sicht der Patientinnen und Patienten unbefriedigend ist. Diese sollen nachvollziehen können, wer zugriffsberechtigt ist bzw. wer auf ihre Daten zugegriffen hat, und müssen Personen, die von einer Gruppenberechtigung erfasst sind, auf eine Ausschlussliste («black list») setzen können. Wir beantragen Ihnen, dieses Thema nochmal aufzunehmen und eine bessere Lösung vorzuschlagen.

Datenschutzrechtliche Aufsicht über die Stammgemeinschaften und Gemeinschaften: In der EPDV sollte festgehalten werden, wer die datenschutzrechtliche Aufsicht über die Stammgemeinschaften und Gemeinschaften hat. Um eine einheitliche Aufsicht sicherzustellen, bietet sich eine generelle Aufsicht des EDÖB an. Aus Sicht der Kantone wäre eine solche Lösung vertretbar.

Verschlüsselung: Die Vorgabe zur Verschlüsselung der Datenhaltung und -übertragung sollte nicht erst in der TOZ, sondern bereits in der EPDV verankert werden. Es handelt sich aus datenschutzrechtlicher Sicht um eine zentrale und zwingende Vorgabe.

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art. 1 Abs. 1	Es sollte zumindest für die Vornahme der Grundeinstellung und als Orientierungshilfe für die Gesundheitsfachpersonen sowie die Patienten und Patientinnen in der Verordnung in beispielhafter Form festgehalten werden, welche Datenarten in etwa unter welche Vertraulichkeitsstufen fallen (z.B. als neuer Absatz 2). Die jeweiligen Datenarten lediglich in den Erläuterungen darzulegen, ist aus datenschutzrechtlicher Sicht ungenügend. Die Erläuterungen werden von jenen, die das elektronische Patientendossier im Alltag anwenden, kaum je gelesen (sofern sie überhaupt wissen, dass es solche gibt). Eine entsprechende Ergänzung drängt sich umso mehr auf, als sich die Zugriffsrechte an den Vertraulichkeitsstufen ori-	***Formulierungsvorschlag:*** Unter die Vertraulichkeitsstufen im Sinne von Absatz 1 fallen insbesondere die folgenden Datenkategorien: a. «nützliche Daten»: Identifikationsangaben zur Patientin/zum Patienten sowie medizinische Grunddaten insbesondere in Form von Patientenverfügungen, Organspenderausweisen sowie Angaben zur Blutgruppe, zu Allergien oder Unverträglichkeiten. b. «medizinische Daten»: behandlungsrelevante Dokumente und Daten zu nicht stigmatisierenden Krankheiten wie z.B. Beinbrüchen, Grippesymptomen, Rückenleiden, Krampfadern usw. c. «sensible Daten»: medizinische Daten, die aus Sicht der Patientin oder des Patienten sensibel sind wie insbesondere Befunde und

	entieren (siehe Art. 2 EPDV).	damit zusammenhängende Behandlungen von stigmatisierenden Krankheiten (z.B. HIV oder psychiatrische Leiden). d. «geheime Daten»: Medizinische Daten, die nach dem Willen der Patientin/des Patienten nur sie oder er einsehen können sollen.
Art. 1 Abs. 2 und Art. 2 Abs. 2	Aus datenschutzrechtlicher Sicht erscheint es aus einem «Privacy by Default»-Ansatz (siehe Erläuterungen Art. 14 Abs. 2) prüfenswert, inwiefern die Grundeinstellungen restriktiver auszugestalten sind. In Art. 1 Abs. 2 wäre entsprechend zu regeln, dass neu eingestellte Daten den «sensiblen Daten» zugewiesen werden und in Art. 2 Abs. 2, dass im Fall einer fehlenden Zuweisung das Zugriffsrecht «eingeschränkt» gilt.	Frage ist zu prüfen.
Art. 2 Abs. 3	Aus «Privacy by Default-Überlegungen sollte die Einräumung von Zugriffsrechten in der Grundeinstellung nicht unbefristet erfolgen. Die Patientin oder der Patient kann anschliessend einzelnen Gesundheitsfachpersonen wie z.B. dem Hausarzt/der Hausärztin immer noch einen unbefristeten Zugriff einräumen. Ein solches Vorgehen bedingt eine Anpassung von Art. 3 lit. a (siehe nachfolgend). Zudem ist eine Informationsmeldung an den Patienten/die Patientin vor Fristablauf der Zugriffsrechte zu prüfen.	***Formulierungsvorschlag:*** [3] Die Zugriffsrechte werden den einzelnen Gesundheitsfachpersonen für längstens zwei Jahre eingeräumt.
Art. 2 Abs. 4	Wenn an Gruppenberechtigungen wie in diesem Absatz beschrieben festgehalten werden soll, dann ist es zwingend, auch an der Regelung von Art. 3 lit. f festzuhalten: Ohne jene Möglichkeit eines «Opt-out» erscheinen Gruppenberechtigungen aus datenschutzrechtlicher Sicht nicht vertretbar.	---
Art. 3 lit. a	Aus «Privacy by Default»-Überlegungen sollte der Zugriff in der Grundeinstellung nicht unbefristet erfolgen. Die Patientin oder der Patient kann anschliessend einzelnen Gesundheitsfachpersonen wie z.B. dem Hausarzt/der Hausärztin immer noch einen unbefristeten Zugriff einräumen.	***Formulierungsvorschlag:*** a. einzelnen Gesundheitsfachpersonen unbefristete Zugriffsrechte einräumen;
Art. 3 lit. f	Siehe Bemerkung zu Art. 2 Abs. 4.	---

Art. 3 lit. h	Ist es zutreffend und gewollt, dass Zugriffsrechte nur an Gesundheitsfachpersonen *innerhalb derselben Stammgemeinschaft* weiter gegeben werden können, nicht aber auch an Gesundheitsfachpersonen anderer Stammgemeinschaften und Gemeinschaften? Falls nicht, dann sollte der Verordnungstext entsprechend angepasst werden. Ergänzend sollte festgehalten werden, dass die Gesundheitsfachperson bei der Zuweisung von Zugriffsrechten an weitere Gesundheitsfachpersonen die Patientin/den Patienten über die entsprechende Zuweisung informieren muss.	***Formulierungsvorschlag:*** 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.
Art. 4	Aus datenschutzrechtlicher Sicht ist zu begrüssen, dass die Patientenidentifikationsnummer so auszugestalten ist, dass sie keinerlei Rückschlüsse auf die Person zulässt.	---
Art. 9 Abs. 1 lit. a	Bei dieser Regelung ist nicht klar, ab wann die genannten zehn Jahre zu laufen beginnen - nach Einstellung des Dokuments ins elektronische Patientendossier, nach der letzten Behandlung in der jeweiligen Sache oder…? Im Weiteren stellt sich die Frage, inwiefern der Patient/die Patientin vor Ablauf der 10 Jahre über die bevorstehende Löschung informiert werden sollte. Falls er oder sie das Dokument nicht gelöscht haben möchte, könnte er/sie dies entsprechend veranlassen.	Diese Fragen sollten geklärt und Art. 9 Abs. 1 lit. a entsprechend ergänzt werden.
Art. 9 Abs. 5	Eine Kann-Vorschrift erscheint hier nicht zielführend. Es sollte eine regelmässige Überprüfung des Stands der Technik stattfinden und bei Veränderungen, die zu einer Bedrohungslage führen könnten, entsprechende Anpassungen vorgenommen werden.	***Formulierungsvorschlag:*** Das Bundesamt für Gesundheit (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.
Art. 11 Abs. 1 lit. d	In der Ausarbeitung der Gesetzgebung zum elektronischen Patientendossier war nie die Rede davon, dass die Primärsysteme direkt an das elektronische Patientendossier angeschlossen werden sollen. Vielmehr wurde ein entsprechender Anschluss der Sekundärsysteme vorgesehen.	Hier ist zu prüfen, ob wirklich ein Anschluss der Primärsysteme stattfinden soll, was aus datenschutzrechtlicher Sicht erheblich problematisch und nicht empfehlenswert erscheint. Wird tatsächlich ein Anschluss der Primärsysteme angestrebt, müssten diese die datenschutz- und informationssicherheitsrechtlichen Vorgaben der EPD-Gesetzgebung erfüllen.

Art. 11 Abs. 4	Da es sich bei Gesundheitsdaten um besonders schützenswerte Personendaten handelt und im Rahmen des ePatientendossiers auch die Gefahr der Entstehung von Persönlichkeitsprofilen besteht, ist diese Regelung aus datenschutzrechtlicher Sicht zwingend. Sie wird entsprechend sehr begrüsst. Es ist jedoch zu prüfen, ob es ausreicht, lediglich den Datenspeicher in der Schweiz zu lokalisieren und diesen Schweizer Recht zu unterstellen. Aufgrund der stetigen Zunahme des extraterritorialen Gebaren gewisser Staaten (z.B. USA) ist prüfen, ob nicht auch der Firmensitz und der Arbeitsplatz aller involvierten Mitarbeitenden (insbesondere auch der IT- und Support-Mitarbeitenden) zwingend in der Schweiz zu sein hat.	---
Art. 14 Abs. 1	Diese Regelung sollte eine Verpflichtung der Stammgemeinschaft vorsehen, die Patientin/den Patienten über mögliche informationssicherheitsrechtliche Risiken der Nutzung des ePatientendossiers aufzuklären.	***Formulierungsvorschlag:*** ***lit. e***…die informationssicherheitsrechtlichen Risiken der Nutzung des elektronischen Patientendossiers.
Art. 14 Abs. 2	Die Datenschutz- und Datensicherheitsmassnahmen sollten dem Patienten/der Patientin nicht empfohlen, sondern durch entsprechende technische Voreinstellungen (z.B. passwortgeschützte Zugänge, zwingende Verschlüsselungen usw.) vorgegeben werden (Privacy by Default). Bei einer reinen Empfehlung wird die Verantwortung an den Patienten/die Patientin abgeschoben, was aufgrund der Art der bearbeiteten Daten nicht angemessen erscheint.	Die Empfehlung sollte durch technische Voreinstellungen ersetzt werden.

Art. 20 Abs. 1 lit. c	Hier erscheint unklar, wie die Stammgemeinschaft vom Tod des Patienten/der Patientin erfährt. Allenfalls ist zu prüfen, inwiefern eine Meldepflicht durch die ZAS zielführend ist. Zudem ist zu prüfen, inwiefern nach dem Tod eines Patienten/einer Patientin für die Löschung eine Übergangsfrist von mehreren Jahren sinnvoll erscheint. Es kann für die Angehörigen aus mehreren Gründen notwendig sein, Zugriff auf das elektronische Patientendossier zu erhalten (z.B. zwecks Analyse des Risikos von Erbkrankheiten, im Fall von Fragen der Zurechnungsfähigkeit des Erblassers/der Erblasserin bei Erbstreitigkeiten usw.) – siehe dazu auch die Regelung von Art. 9 Abs. 1 lit. b.	Diese Fragen sind zu prüfen und Art. 20 Abs. 1 lit. c und Art. 9 Abs. 1 lit. b sind je nach Resultat der Prüfung anzupassen.
3. Abschnitt	Der dritte Abschnitt sollte um einen Artikel erweitert und der Abschnittstitel entsprechend angepasst werden.	***Formulierungsvorschlag:*** ***Datenbearbeitungszwecke, Datenlieferung für die Evaluation***
Neuer Art. 20bis *(im 3. Abschnitt vor Art. 21)*	Es sollte ausdrücklich festgehalten werden, dass alle am Aufbau, dem Betrieb oder der Nutzung des EPD Beteiligten, die im Zusammenhang mit dem EPD anfallenden Personendaten lediglich zur Erfüllung der ihnen durch das EPDG oder einen damit verbundenen Erlass übertragenen Aufgaben (oder allenfalls gestützt auf eine andere hinreichend bestimmte gesetzliche Grundlage) bearbeiten dürfen. Zwar lässt sich ein solches Verbot aus Art. 4 Abs. 3 DSG ableiten. Aufgrund der Art der im Zusammenhang mit dem elektronischen Patientendossier anfallenden Personendaten (besonders schützenswerte Personendaten, Persönlichkeitsprofile) erscheint es jedoch angemessen, eine entsprechende Regelung explizit in die EPDV aufzunehmen.	***Formulierungsvorschlag:*** [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.
Bisheriger Art. 21	Diese Regelung muss aus datenschutzrechtlicher Sicht präzisiert werden. Das BAG sollte nur berechtigt sein, die Daten in anonymisierter Form zu bearbeiten. Die Auflistung in Anhang 6 der EPDV-EDI verdeutlicht, dass anonymisierte Daten für die Erhebung der beabsichtigten Informationen problemlos ausreichen.	***Formulierungsvorschlag:*** ***Art. 21*** Abs. 1: Wie bisher Abs. 2: 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 anonymisieren zu

		lassen. Abs. 3: Das EDI legt die zu liefernden Daten fest.
Art. 22 lit. d	Eine Gültigkeit von höchstens zehn Jahren scheint in Anbetracht der stets voranschreitenden Weiterentwicklung der Technik sehr lang. Den Erläuterungen lassen sich zu diesem Punkt leider keine Hintergrundüberlegungen entnehmen.	Die Maximalfrist von zehn Jahren sollte überprüft werden. Allenfalls wäre es zielführender, diese auf zwei Jahre festzusetzen.
Art. 33	Die Regelung von Absatz 1 (jährliche Überprüfung) ist aus datenschutzrechtlicher Sicht sehr zu begrüssen.	---
Art. 36	Es ist zu überprüfen, ob eine «Kann-Vorschrift» hier tatsächlich zielführend ist. Wenn eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vorliegt, sollte das BAG handeln müssen.	***Formulierungsvorschlag:*** Liegt eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten 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 Identifikationsmittel; c. ordnet eine ausserordentliche Rezertifizierung an.
Art. 37 Abs. 1	Eine «Kann-Vorschrift» erscheint beim Vorliegen schwerer Mängel nicht angemessen. Vielmehr gilt es die Zertifizierungsstelle beim Vorliegen von schweren Mängeln zu verpflichten, die Gültigkeit des Zertifikats auszusetzen oder das Zertifikat zu entziehen.	Art. 37 Abs. 1 sollte entsprechend angepasst werden.
Art. 37 Abs. 3	Da die Entscheidungsbehörde das BAG ist, kommt das Verwaltungsverfahren zur Anwendung (Art. 1 VwVG, SR 172.021). In diesem Zusammenhang sollte geprüft werden, ob das Verwaltungsverfahren hier die notwendigen Handlungsfreiheiten bzgl. Schnelligkeit, Effektivität usw. zu gewährleisten vermag.	Prüfen, ob das Verwaltungsverfahren hier zielführend ist.

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

Allgemeine Bemerkungen

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art. 6	Dieser Artikel ist um die Vorgabe zu ergänzen, dass die Gemeinschaften die entsprechenden Daten dem BAG nur in anonymisierter Form liefern dürfen. Aus den in Anhang 6 aufgeführten Daten ergibt sich, dass dies für die geplanten Auswertungen ausreicht.	***Formulierungsvorschlag: Einfügen von Abs. 2:*** [2] Die Gemeinschaften und Stammgemeinschaften sind verpflichtet, die Daten vor der Weiterleitung an das BAG zu anonymisieren oder anonymisieren zu lassen.

Bemerkungen zu den Erläuterungen

Seite / Artikel	Kommentar	Änderungsantrag