Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Verbraucherschutz

Stellungnahme zur Vernehmlassung der Revision des EPDG: Umfassende Revision EPDG
Prise de position concernant la consultation sur la révision complète de la LDEP
Modulo per parere sulla consultazione concernente la revisione della LCIP (revisione completa)

Stellungnahme von / Prise de position de / Parere di:

Name, Kanton, Firma, Organisation: Nom, canton, entreprise, organisation : Nome, Cantone, ditta, organizzazione:	**Information Security Society Switzerland, Bern**
Abkürzung der Firma, Organisation: Abréviation de l'entreprise, l'organisation : Abbreviazione della ditta, dell'organizzazione:	ISSS
Adresse, Ort: Adresse, lieu : Indirizzo, località:	Zentweg 13, 3006 Bern
Datum / Date / Data:	

Frist zur Einreichung der Stellungnahme: **19. Oktober 2023**
Délai pour le dépôt de la prise de position : **19 octobre 2023**
Termine per la presentazione del parere: **19 ottobre 2023**

Hinweise

1. Bitte das Deckblatt mit Ihren Angaben ausfüllen.
2. Pro Artikel (Gesetz/Verordnung) oder Ziffer (erläuternder Bericht) eine eigene Zeile verwenden.
3. Ihre elektronische Stellungnahme senden Sie bitte als **Word-Dokument** bis am **19. Oktober 2023** an: ehealth@bag.admin.ch und gever@bag.admin.ch

Indications

1. Veuillez remplir la page de garde avec vos coordonnées.
2. Veuillez utiliser une ligne pour chaque article (loi/ordonnance) ou chiffre (rapport explicatif).
3. Veuillez envoyer votre prise de position électronique au **format Word** d'ici au **19 octobre 2023** aux adresses suivantes: ehealth@bag.admin.ch et gever@bag.admin.ch

Indicazioni

1. Compilare la presente pagina di copertina con i propri dati.
2. Utilizzare una riga separata per ciascun articolo (legge/ordinanza) o numero (rapporto esplicativo).
3. Inviare il parere in **formato Word** per e-mail entro il **19 ottobre 2023** a ehealth@bag.admin.ch e gever@bag.admin.ch

Bundesgesetz über das elektronische Patientendossier (EPDG; SR *816.1*)
Loi fédérale sur le dossier électronique du patient (LDEP; RS *816.1*)
Legge federale sulla cartella informatizzata del paziente (LCIP; RS *816.1*)

Allgemeine Bemerkungen
Remarques générales
Osservazioni generali

Sehr geehrte Damen und Herren

ISSS bedankt sich für die Gelegenheit, im Rahmen der Totalrevision des Gesetzes über das elektronische Patientendossier Stellung nehmen zu können.

Die Information Security Society Switzerland (ISSS; http://www.isss.ch) ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander.

Die Stellungnahme konzentriert sich auf diejenigen Punkte der Vorlage zur umfassenden Revision des Bundesgesetzes über das elektronische Patientendossier, welche im Zusammenhang mit der ICT-Sicherheit und dem Datenschutz stehen.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung des Schutzes von Persönlichkeit und Privatsphäre sowie der ICT-Sicherheit und dem Informationsschutz im Medizinalbereich der Schweiz leisten können und danken Ihnen für die Berücksichtigung unserer Anträge.

An der ISSS Stellungnahme haben folgende ISSS Mitglieder mitgearbeitet:

Dario Walder, ISSS Vizepräsident
Andrea Michel, ISSS Geschäftsführerin
RA lic. iur. Nicole Beranek Zanon, Exec. MBA HSG, CIPP/E, ISSS Vorstand
Petra Breiting, ehem. ISSS Vorstand
Stefan Joos, RUAG
Rico Köchli, Computer Controls AG
Beat Lehmann, ISSS Vorstand
Reto Steinmann, Swiss Infosec AG

Freundliche Grüsse

Dario Walder, ISSS Vizepräsident
Andrea Michel, ISSS Geschäftsführerin

Bemerkungen zu einzelnen Artikeln
Commentaires concernant les différents articles
Osservazioni sui singoli articoli

Artikel **Article** **Articolo**	**Antrag** **Proposition** **Richiesta**	**Begründung / Bemerkung** **Justification / Remarques** **Motivazione / Osservazioni**
-	Generelle Bemerkungen	• Die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der (Patienten-)Daten wird nicht erwähnt, sollte aber im Gesetz erwähnt werden. Alternativ kann auf das ISG und DSG referenziert werden. • Ein Notfallzugang zum EPD, der sich auf die vom Patienten zum Voraus für diese Situationen, z.B. Unfälle, bezeichneten Daten beschränkt und bisher nicht geregelt ist, muss ebenfalls einheitlich geregelt werden. • Die Ausweitung auf medizinischen Daten und administrative Daten sowie den Zugriff der Versicherer birgt das Risiko in sich, dass unverhältnismässig viele medizinische Daten gesammelt und genutzt werden.

		• Ein Hinweis auf die Löschung der Daten im EPD nach der gesetzlichen Aufbewahrungsfrist fehlt gänzlich und ist zu ergänzen. Insbesondere sollte eine Löschung nach Todesfall + x Jahren genannt werden. • Die Unabhängigkeit der Registrier- und Verwaltungsstellen für das EPD und ihre Sicherheitsstruktur (Stammgesellschaften) muss gewahrt werden. Eine Startgenehmigung (nicht notwendigerweise Zertifizierung) für Stammgesellschaften und eine jährliche Kontrolle sind notwendig. • Das EPD als Instrument der obligatorischen Krankenversicherung und eine allfällig damit einhergehende Pflicht zur Verwendung des EPD sehen wir als nicht zielführend. Die Eröffnung soll durch den Patienten beantragt werden müssen und die Möglichkeit eines Opting-Out's soll unbefristet bestehen bleiben. • Patientendaten sind besonders schützenswerte Personendaten, auf die weder die Pharmaindustrie noch die Forschung Zugriff haben dürfen. Forschung und Pharmaindustrie dürfen nur mit ausdrücklicher Genehmigung des Patienten auf seine, von ihm explizit definierten Daten zugreifen
Art. 2	a. elektronisches Patientendossier: virtuelles Dossier, das dezentral und zentral abgelegte medizinische und administrative Daten einer Patientin oder eines Patienten enthält;	Die Begriffe medizinische Daten und administrative Daten sind zu definieren. Medizinische und administrative Daten sind zu trennen. Zugriffsberechtigungen müssen dediziert auf medizinische oder administrative Daten vergeben werden können.
Art. 2	b. Gesundheitsfachperson: nach eidgenössischem oder kantonalem Recht anerkannte Fachperson, die im Gesundheitsbereich Behandlungen durchführt oder anordnet oder im Zusammenhang mit einer Behandlung Heilmittel oder andere Produkte abgibt sowie die für die Beurteilung der Tauglichkeit für den Militärdienst zuständigen Personen nach dem Militärgesetz vom 3. Februar 19953;	Wenn überhaupt der Zugriff auf das EPD zur Beurteilung der Tauglichkeit für den Militärdienst notwendig ist, muss dieser befristet erfolgen, d.h. nur möglich sein, während der Zeit in der die Person Militär- oder Zivildienst leistet.
Art. 3 Abs b	Automatische Eröffnung	Keine automatische Eröffnung eines Patientendossiers. Damit werden wesentliche durch die Verfassung (Art. 5 BV, staatliches Handeln; Art. 7 BV

		Menschenwürde; Art.10 Abs. 2 BV persönliche Freiheit; Art. 11 BV Garantie des besonderen Schutzes von Kindern und Jugendlichen; Art.13 BV Schutz der Privatsphäre: Art.29 Abs. 2 BV Rechtliches Gehör; Art. 35 BV Verwirklichung der Grundrechte) garantierten Rechtsstaatlichkeit unseres verletzt. Ein Widerspruch gegen die Eröffnung des EPD soll sowohl beim Kanton als auch der Stammgemeinschaft möglich sein. Die Rechtssituation bei Patienten mit Beistand, bevormundeten oder verbeiständeten, in psychiatrischen Einrichtungen, in Schutzeinrichtungen, Strafvollzugsanstalten ist nicht aufgeführt. Dies ist u.E. zwingend erforderlich.
Art. 4 Abschnitt 2	Elektronische Patientenidentifikationsmittel	Aus unserer Sicht könnte und sollte anstelle der Patientenidentifikationsnummer die Verwendung der e-ID als Identifikationsmittel benutzt werden. Die Rechtssituation bei Patienten mit Beistand, bevormundet, verbeiständeten, in psychiatrischen Einrichtungen, in Schutzeinrichtungen, Strafvollzugsanstalten ist nicht aufgeführt. Dies ist u.E. zwingend erforderlich
Art. 9	Art. 9*a* 1 Die Krankenversicherer können mit Einwilligung der Patientinnen und Patientenadministrative Dokumente im Zusammenhang mit der Durchführung der obligatorischen Krankenpflegeversicherung sowie der Zusatzversicherung im elektronischen Patientendossier speichern. *Krankenversicherer haben keinen Zugriff auf medizinische Daten.*	Es bedarf einer Konkretisierung resp. Ergänzung. Aus unserer Sicht darf aus datenschutzrechtlicher Sicht den Krankenkassen keinen Zugriff auf medizinische Daten gewährt werden. Ein Zugriff von Krankenkassen soll - sofern überhaupt - erst in einer zweiten Etappe und nur für einen beschränkten Kreis z.B. einem Vertrauensarzt eingeführt werden, nachdem die Zugriffsberechtigungen der verschiedenen Gesundheitsfachpersonen erste Erfahrungen vorliegen und die Akzeptanz des EPD in der Bevölkerung erreicht ist.

	Art. 9c Die Patientin oder der Patient kann bei ihrer beziehungsweise seiner Stammgemeinschaft jederzeit ohne Angabe von Gründen die Auflösung ihres oder seines elektronischen Patientendossiers beantragen. Die im elektronischen Patientendossier enthaltenen Daten werden daraufhin vernichtet.	Präzisieren, was vernichten von Daten bedeutet. Es ist eine dauerhafte Vernichtung ist vorzusehen.
Artikel 10 Abs 2 b	2 Stammgemeinschaften müssen zusätzlich den Patientinnen und Patienten die Möglichkeit geben: b. eigene Daten zu erfassen,	Konkretisierung, welche Daten vom Patienten selber erfasst, geändert und gelöscht werden können, wie z.B. Namensänderungen, Wohnsitzänderungen, Anzahl Kinder, zusätzliche Gesundheitsdaten. Die Rechtssituation bei Patienten mit Beistand, vorübergehend bevormundet, in psychiatrischen Einrichtungen, in Schutzeinrichtungen, Strafvollzugsanstalten ist nicht aufgeführt – zwingend erforderlich
Artikel 11 Abs 1 c	Zertifizierungspflicht c. die Herausgeber von Identifikationsmitteln, mit Ausnahme der Behörden des Bundes.	Konkretisierung des Begriffs “Behörden”. Jegliche Organisation, welche ein EPD betreibt oder auf ein solches zugreift, muss durch den Bund zertifiziert werden. Eine staatliche Anerkennung reicht nicht aus. Ausserdem soll die Zertifizierung regelmässig (z.B. alle drei Jahre) erneuert werden. Allerdings würden diese aus Gründen von Datenschutz und ICT-Sicherheit notwendige Anforderungen die Kosten des EPD nach dem Revisionsvorschlag vermehren.
Artikel 12 und 13	Zertifizierungsverfahren / Zertifizierungsvoraussetzungen	Wir gehen davon aus, dass das bisher durch Art. 11 ff EPDG und Art.30 ff EPDV ausführlich geregelte Zertifizierungsverfahren auch bei der Totalrevision des EPDG erhalten bleibt.
Art. 19	Art. 19 Abs. 1–2bis 1 Der Bundesrat kann die folgenden Aufgaben auf Organisationen und Personen des öffentlichen oder privaten Rechts übertragen	Kontrollmechanismus: Der Bund soll Datenschutz und ICT-Sicherheit nicht nur initial, sondern regelmässig überprüfen. Ein entsprechender Artikel soll verfasst und im Gesetz verankert werden.

Art. 19	**2bis Der Bund schliesst mit den beigezogenen Dritten einen Leistungsauftrag ab. Darin ist insbesondere Folgendes festzulegen:** **a. Art, Umfang und Abgeltung von Leistungen, die von den Dritten zu erbringen sind;** **b. die Modalitäten für eine periodische Berichterstattung, Qualitätskontrolle,Budgetierung und Rechnungslegung;** **c. die allfällige Erhebung von Gebühren** **d. die Anforderung an den Datenschutz und ICT-Sicherheit**	Art. 19 Abs 2 b: Genaue Zielvorgaben bezüglich Nutzen und Aufwand müssen definiert und zentral von einer Behörde kontrolliert werden. Diese Zielvorgaben müssen aus unserer Sicht sowohl den Nutzen als auch den Aufwand in Betracht ziehen. Zudem sollte aus unserer Sicht von einem Leistungsauftrag abgesehen und ein verwaltungsrechtlicher Vertrag mit einer längerfristigen Dauer abgeschlossen werden, damit eine langfristige Schutz-Perspektive gewährleistet werden kann. Art. 19 Abs d Konkretisierung ist zwingend notwendig. Im EPD sind sowohl die Vertraulichkeit der Daten, die Integrität der Daten aber auch die zeitnahe Verfügbarkeit (beispielsweise bei einem Notfall) von grosser Wichtigkeit. Dies soll entsprechend ausformuliert und nicht nur mit einem Satz umschrieben werden.