DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Departement des Innern EDI
Inselgasse 1
3003 Bern

Per E-Mail an: ehealth@bag.admin.ch
Sowie an: gever@bag.admin.ch

19. Oktober 2023

Stellungnahme zur umfassenden Revision des Bundesgesetzes über das elektronische Patientendossier (2022/97)

Sehr geehrte Damen und Herren

Am 28. Juni 2023 eröffnete der Bundesrat die Vernehmlassung zur umfassenden Revision des Bundesgesetzes über das elektronische Patientendossier (EPDG; SR 816.1). Wir danken Ihnen für die Möglichkeit am Vernehmlassungsverfahren teilzunehmen.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Entwurf wie folgt Stellung.

Vorbemerkung und Zusammenfassung

Die Digitale Gesellschaft anerkennt die Notwendigkeit einer Revision des Bundesgesetzes über das elektronische Patientendossier (EPDG). Das EPD konnte sich bis anhin nicht durchsetzen. Auf Seiten der Leistungserbringer war und ist die Einführung mit viel Aufwand und hohen Kosten bei wenig Nutzen verbunden. Für die Patientinnen und Patienten besteht keinen Anreiz, ein Dossier zu eröffnen, wenn es vom Leistungserbringer (da noch nicht angeschlossen) nicht befüllt wird, es kompliziert in der Handhabung ist und das Potential für einen Datenmissbrauch (siehe weiter

unten) beträchtlich ist. Verschiedene Sicherheitslücken und Datenabflüsse, die in jüngster Zeit bekannt wurden, und die auch das Gesundheitswesen und den Bund betrafen, konnten das Vertrauen nicht eben fördern.

Die Schlüsse, die der Bundesrat aus der gescheiterten Einführung zieht, sind nach Ansicht der Digitalen Gesellschaft falsch. Das EPD muss in erster Linie den Menschen ins Zentrum stellen und ihm einen konkreten Nutzen bringen. Es muss benutzerfreundlich und sicher sein. Das Produkt muss für sich überzeugen. Die Abschaffung der Freiwilligkeit (Opt-In) führt hingegen dazu, dass diese «Hausaufgaben» vernachlässigt werden (können) und sorgt durch die «Zwängerei» für einen Vertrauensverlust.

Erst in zweiter Linie sollte das EPD die Forschung und Qualitätssicherung im Gesundheitswesen adressieren. Beides sind keine Aufgaben, die durch ein EPD in seiner personalisierten Form geleistet werden können. Bei Gesundheitsdaten handelt es sich gemäss Datenschutzgesetz (DSG) um besonders schützenswerte Personendaten. Ein Zugriff darauf oder eine Weitergabe dieser Daten bedarf bei einer benötigten Einwilligung besonders hohen Anforderungen. Bei einer sogenannten «Sekundärnutzung» von Daten für Forschung oder für statistische Analysen im Gesundheitswesen werden zusammengeführte Datensätze benötigt. Die Daten dafür könnten (und müssten) komplett anonymisiert bearbeitet werden. Eine solche Nutzung kann im Rahmen vom EPDG geregelt werden, könnte aber auch ausserhalb dieses Gesetzes umgesetzt werden.

Die Digitale Gesellschaft befürwortet die Digitalisierung im Gesundheitswesen, lehnt aber die umfassende Revision des Bundesgesetzes über das elektronische Patientendossier (EPDG) in der vorliegend Form aus folgenden Gründen zusammenfassend ab:

- Die Abschaffung der Freiwilligkeit (Opt-In) für die Patientinnen und Patienten steht im Widerspruch zur informationellen Selbstbestimmung, welche durch die Bundesverfassung in Art. 13 Abs. 2 garantiert ist.
- Die im Gesetz kolportierte «dezentrale» Datenspeicherung ist in der Praxis eine zentrale Datenhaltung, die nicht dem datenschutzrechtlichen Grundprinzip von Privacy-by-Design (Datenschutz durch Technikgestaltung) entspricht.
- Das Anlegen und Pflegen von über 4 Millionen ungenutzten Dossiers ist nicht nur ökonomisch unsinnig sondern stellt auch ein enormes Datenmissbrauchsrisiko dar.

Wir fordern den Bundesrat daher auf, eine Totalrevision des Bundesgesetzes über das elektronische Patientendossier (EPDG) nach den genannten Prinzipien (Nutzen und

Freiwilligkeit für die Menschen; sichere, dezentrale und datensparsame Datenhaltung) anzugehen und sind überzeugt, dass ein sicheres und vertrauenswürdiges EPD auch die nötige Verbreitung findet, um nicht nur die Qualität in Behandlung, Nachsorge oder Forschung zu verbessern, sondern auch zu Kosteneinsparungen im Gesundheitswesen beizutragen.

Bundesgesetz über das elektronische Patientendossier

Dezentral versus zentral abgelegte medizinische und administrative Daten (Art. 2 lit. a, Art. 14 VE-EPDG)

Neu einführen möchte der Bundesrat eine «zentrale» Datenbank zur Speicherung von strukturierten Gesundheitsdaten von Patientinnen und Patienten. Bei diesen Daten soll es sich um Vitaldaten (wie Blutdruck), Laborwerte, aber auch Medikationsdaten handeln, die sich dynamisch über die Zeit ändern. Der Entwurf überlässt es dem Bundesrat, zu definieren, welche Daten strukturiert und zentral abgelegt werden sollen. Nach Ansicht der Digitalen Gesellschaft sollte jedoch bereits auf Gesetzesstufe festgelegt werden, welche Datenkategorien in der zentralen Datenbank abgelegt und wie diese dann von wem bearbeitet werden dürfen.

Der erläuternde Bericht zum Vorentwurf schreibt, dass bisher «sämtliche Daten dezentral bei den Gemeinschaften und Stammgemeinschaften gespeichert» worden seien. Er verschweigt dabei die Tatsache, dass von der ursprünglichen Idee, dass in der Schweiz 20 bis 40 Stammgemeinschaften entstehen sollen, welche die Daten aus «einer bestimmten Region, eines bestimmten Kantons oder mehrerer Kantone» verwalten (vgl. Botschaft zum EPDG vom 29. Mai 2013), nicht mehr viel übrig geblieben ist. Mit der Übernahme von Axsana durch die Schweizerische Post, ist diese nun die technische Anbieterin von elektronischen Patient:innendossiers in allen 26 Kantonen.

Doch auch die Speicherung der Gesundheitsdaten bei – und unter der Kontrolle von – 20 bis 40 Stammgemeinschaften ist keine dezentrale Datenhaltung. Dezentrale Datenhaltung bedeutet die Speicherung der Daten bei der betroffenen Person, resp. im Falle des EPD unter der Kontrolle (durch Verschlüsselung) der betroffenen Person. Die Einhaltung des datenschutzrechtlichen Grundprinzips von Privacy-by-Design (Datenschutz durch Technikgestaltung) würde bedeuten, dass zunächst ausschliesslich die betroffene Person sowie die Gesundheitsfachperson (resp. die leistungserbringende Organisation), welche die Daten einstellt, die entsprechenden Daten bearbeiten können. Verschlüsselung verhindert dabei, dass sich andere Personen und Personengruppen (wie auch die Anbieterin des EPD selbst), Zugang

verschaffen können, ohne dass sie von der betroffenen Person berechtigt worden wären.

Einwilligung zur Erstellung eines elektronischen Patientendossiers (Art. 3 VE-EPDG)

Das aktuell geltende Recht sieht in Art. 3 vor: «Für die Erstellung eines elektronischen Patientendossiers ist die schriftliche Einwilligung der Patientin oder des Patienten erforderlich. Die Einwilligung ist nur gültig, sofern die betroffene Person sie nach angemessener Information über die Art und Weise der Datenbearbeitung und deren Auswirkungen freiwillig erteilt.» Gemäss erläuterndem Bericht zum Vorentwurf war der Leitgedanke zur Bestimmung, «dass jede Person im Sinne der informationellen Selbstbestimmung selbst entscheiden können soll, ob sie ein EPD eröffnen möchte und falls sie ein EPD eröffnet hat, ob sie ihren Gesundheitsfachpersonen umfassende oder beschränkte oder keine Zugriffsrechte erteilen will». Dieser Leitgedanke und die Selbstbestimmung sollen nun nicht mehr gelten. Vielmehr soll gemäss Vorentwurf für jede Person automatisch ein Dossier angelegt werden.

Die informationelle Selbstbestimmung ist durch Art. 13 Abs. 2 der Bundesverfassung garantiert. Als Grund für die Einschränkung wird die mangelnde Verbreitung des EPD angeführt. Gemäss erläuterndem Bericht würde dennoch dem Recht auf informationelle Selbstbestimmung Rechnung getragen: «Für die Einwohnerinnen und Einwohner bleibt die Teilnahme letztendlich freiwillig, da eine Widerspruchslösung gilt (Opt-out Modell). Das heisst, wer kein EPD möchte, muss dies aktiv mitteilen, ansonsten wird Zustimmung angenommen.»

Gemäss Datenschutzgesetz gehören Gesundheitsdaten zur Kategorie der besonders schützenswerten Personendaten. Die Daten werden Dritten (einer Stammgemeinschaft und deren Technologie-Anbieterin sowie der Anbieterin der zentralen Datenbank) bekanntgegeben. Daher muss bei der Bearbeitung von Gesundheitsdaten im EPD sogar von einer Persönlichkeitsverletzung ausgegangen werden. Die mangelnde Verbreitung von Dossiers kann dabei nicht als Rechtfertigung dienen, die besonders schützenswerten Personendaten dennoch zu bearbeiten.

Die Einführung eines Opt-out-Modells ist auch nicht, wie der erläuternde Bericht zum Vorentwurf schreibt, «das mildeste Mittel, um die Verbreitung des EPD möglichst rasch sicherzustellen». Erstens heiligt der Zweck nicht das Mittel. Und zweitens muss das elektronische Patient:innen-Dossier für die Betroffenen einen Nutzen bringen und benutzerfreundlich sein. Sicherheit und Funktionalität des Produktes müssen überzeugen. Ein Zwang zum Dossier hingegen führt nicht zum nötigen Vertrauen. Im Gegenteil: Ein Datenverlust von Gesundheitsdaten von Millionen von Menschen, die einem Dossier nie zugestimmt haben, (siehe nachfolgend) würde das Vertrauen in die

staatliche Datenbearbeitung massiv und nachhaltig beeinträchtigen.

Am Opt-In-Prinzip, also der Freiwilligkeit der Eröffnung und Nutzung eines Dossiers für Patientinnen und Patienten, ist in Art. 3 festzuhalten.

Widerspruch gegen die automatische Eröffnung (Art. 3a, Art. 9 Abs. 1bis VE-EPDG)

Gemäss der zum Vorentwurf veröffentlichten Regulierungsfolgenabschätzung muss mit ca. 3 Prozent Widersprüchen wie in Österreich gerechnet werden: «Damit sollten nach der einjährigen Übergangsfrist im Jahr 2029 rund 9.2 Mio. Personen über ein EPD verfügen. Zum andern ist aber mit einer substanziellen Zahl inaktiver EPD von Personen zu rechnen, die keinen Widerspruch eingelegt haben, das EPD aber trotzdem nicht nutzen. Schätzungen der befragten Akteure liegen im Durchschnitt bei 40 bis 45 Prozent inaktiver, Betriebskosten verursachenden Dossiers. In diesen werden besonders schützenswerte Gesundheitsdaten durch die GFP [Gesundheitsfachpersonen] abgelegt, ohne dass die Patientinnen und Patienten aktiv Widerspruch eingelegt haben.»

Daraus lässt sich folgendes schliessen

1. Das Widerspruchsrecht muss von den betroffenen Personen einfach wahrgenommen werden können, wie es die Regulierungsfolgenabschätzung vorschlägt. Art. 3a VE-EPDG ist entsprechend zu ergänzen.
2. Das Pflegen von 4 Millionen Dossiers von Personen, die es weder aktiv noch passiv nutzen, ist nicht nur ökonomisch unsinnig sondern stellt ein enormes Risiko für Datenmissbrauch dar. Dies stellt auch die Regulierungsfolgenabschätzung entsprechend fest: «Eine grössere Menge an Gesundheitsdaten wird zu einem interessanten Ziel für Cyberangriffe. Gleiches gilt für die zentrale Ablage, wenn alle Daten an einem Ort gespeichert sind.»
3. In diesen 4 Millionen EPDs sind noch nicht jene enthalten, die wohl von den Patient:innen «eröffnet» worden sind, aber nicht (mehr) aktiv verwendet werden, weil beispielsweise der Nutzen oder die Benutzerfreundlichkeit für die Betroffenen nicht gegeben ist oder auch die Zugangsdaten nicht mehr verfügbar sind.

Nach dem Festgestellten ist nicht nachvollziehbar, wieso gemäss Regulierungsfolgenabschätzung gut kommuniziert werden muss, «dass ein Opt-out zur Löschung sämtlicher Daten im Dossier führt und der Vorteil eines inaktiven Dossiers, welches zukünftig mal die Daten nutzbar macht, unwiederbringlich erlischt». Es ist im Gegenteil Art. 9 Abs. 1bis dahingehend anzupassen, dass nachträglich und auf Wunsch die relevanten Daten nachgetragen werden müssen.

Identifikationsmittel (Art. 7 VE-EPDG)

Vor dem Hintergrund der Volksabstimmung zur E-ID erstaunt die Vorgabe, dass die Wahl der «Identifikationsmittel» den Stammgemeinschaften überlassen werden soll, diese von den Stammgemeinschaften auch selbst herausgegeben werden können und «nicht zwingend durch einen anerkannten Herausgeber von Identifikationsmitteln (Identity Provider; IdP) bereitgestellt werden» müssen. So haben am 10. März 2021 fast zwei Drittel der Stimmberechtigten einer privaten E-ID – und damit den genannten IdP – doch eine deutliche Abfuhr erteilt.

Die abgelehnte E-ID war auch für den Zugriff auf das EPD vorgesehen. Es besteht nun jedoch keine Veranlassung den Begriff «elektronische Identität» in «elektronisches Identifikationsmittel» umzubenennen, um «Verwechslungen mit der geplanten E-ID des Bundes» zu vermeiden. Vielmehr soll eine neue E-ID (ausgestaltet nach den Grundsätzen Privacy-by-Design, Datensparsamkeit und dezentrale Datenspeicherung) für den Zugriff auf das EPD (neben anderen, bestehenden Lösungen) zwingend (für die Stammgemeinschaften) verwendet werden können. Art. 7 VE-EPDG ist entsprechend anzupassen.

Gesundheitsanwendungen für Patientinnen und Patienten (Art. 9b VE-EPDG)

Eine zusätzliche Schnittstelle für Gesundheitsanwendungen schafft einen zusätzlichen Angriffsvektor und erhöht damit das Risiko für einen Missbrauch der Daten. Daher sollte ein Zugriff auf das EPD über eine solche Schnittstelle – wenn überhaupt – dann nur sehr eingeschränkt möglich sein. Eine solche Einschränkung darf sich nicht nur auf entsprechende Zugriffsrechte beschränken, vielmehr sind die Daten aus dem EPD (die von den Gesundheitsfachpersonen gepflegt werden) von den Daten aus den Gesundheitsanwendungen technisch zu trennen, damit bei einem Missbrauch nicht sämtliche Daten aus dem Dossier mit betroffen sind. Entsprechend hoch müssen auch die Anforderungen an das «Identifikationsmittel» sein. Art. 9b VE-EPDG ist entsprechend anzupassen.

Unterstützung durch den Bund (Art. 19a, Art. 14a VE-EPDG)

Software, die der Bund selbst entwickelt oder die mit Finanzhilfen des Bundes entwickelt werden, müssen nachhaltig und nach dem Leitgedanken «Public money? Public code!», wie es auch das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) in Art. 9 im Grundsatz vorsieht, unter einer anerkannten Open Source Lizenz veröffentlicht werden. Dies ist im Gesetz in Art. 19a entsprechend festzuschreiben.

Datenbekanntgabe (Art. 19g VE-EPDG)

Die Daten zur Forschung und Qualitätssicherung, welche der Bund in anonymisierter Form bekannt gibt, müssen zwingend den Anforderungen an die Anonymisierung nach dem neusten Stand der Technik entsprechen. Auf die entsprechende Bestimmung in Art. 19g VE-EPDG darf nicht verzichtet werden.

Pilotprojekte (Art. 19h Abs. 4 VE-EPDG)

Aufgrund der potenziell weitreichenden Konsequenzen sollte nur der Bundesrat (anstelle dem Eidgenössischen Departement des Innern) die Kompetenz erhalten, in einer Verordnung Abweichungen vom EPDG und von dessen Ausführungsbestimmungen für Pilotprojekte festlegen zu dürfen. Art. 19h Abs 4 VE-EPDG ist entsprechend anzupassen.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter