Kanton Zürich
Gesundheitsdirektion
Recht

Marius Kobi, lic. iur. LL.M.,
Rechtsanwalt
Stampfenbachstrasse 30
Postfach
8090 Zürich
Telefon +41 43 259 24 64
Fax +41 43 259 51 63
marius.kobi@gd.zh.ch
www.gd.zh.ch

238-2011 / 1006-04-2016 / McK

An die Adressaten gemäss Verteiler

18. April 2016

Untervernehmlassung zum Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier (EPDG)

Sehr geehrte Damen und Herren

Das eidgenössische Departement des Innern (EDI) hat mit Schreiben vom 22. März 2016 die Anhörung zum Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier eröffnet. Wir laden Sie ein, bis Mittwoch, 18. Mai 2016, zum Ausführungsrecht Stellung zu nehmen.

1. Auswirkungen des Ausführungsrechts auf den Kanton und die Leistungserbringer

Das Bundesgesetz über das elektronische Patientendossier (EPDG) weist den Gemeinschaften (organisatorische Einheit von Gesundheitsfachpersonen und deren Einrichtungen) und Stammgemeinschaften (Gemeinschaft, die zusätzliche Aufgaben übernimmt) eine wesentliche Rolle zu: Gemeinschaften müssen sicherstellen, dass Daten im Sinne von Art. 3 Abs. 2 EPDG über das elektronische Patientendossier zugänglich sind und dass jede Bearbeitung von Daten protokolliert wird (Art. 10 Abs. 1 EPDG). Stammgemeinschaften müssen u.a. zusätzlich den Patientinnen und Patienten die Möglichkeit geben, auf ihre Daten zuzugreifen und eigene Daten im elektronischen Patientendossier zu erfassen (Art. 10 Abs. 2 lit. b EPDG). Es braucht eine Stammgemeinschaft, damit Patientinnen und Patienten auf das elektronische Patientendossier zugreifen können.

Leistungserbringer, die stationäre Leistungen erbringen, sind verpflichtet, sich einer Gemeinschaft oder Stammgemeinschaft anzuschliessen (Rechtsgrundlage: mit Art. 25 EPDG wird in Art. 39 Abs. 1 KVG, der die Zulassung von Leistungserbringern regelt, eine entsprechende lit. f eingefügt werden). Der Bund plant, das EPDG und sein Ausführungsrecht auf den 1. Januar 2017 in Kraft zu setzten. Gemäss Übergangsbestimmungen zum EPDG haben Spitäler drei Jahre Zeit, sich einer Gemeinschaft oder Stammgemeinschaft anzuschliessen; den Geburtshäusern und Pflegeheimen wird eine Übergangsfrist von 5 Jahren gewährt. Spitäler müssen somit das EPDG und sein Ausführungsrecht bis spätestens zum 1. Januar 2020, Geburtshäuser und Pflegeheime bis zum 1. Januar 2022 umgesetzt haben.

Der personelle, organisatorische und technische Aufwand, den die Spitäler, Rehabilitationskliniken, Geburtshäuser und Pflegeheime für die Umsetzung des Ausführungsrechts erbringen müssen, dürfte erheblich sein.

Weder das EPDG noch das Ausführungsrecht verpflichten die Kantone zur Mitwirkung. Dennoch besteht für den Kanton Handlungsbedarf: Das EPD soll zum Schutz der Gesundheit, zur Gesundheitsförderung, zur Prävention und zur Stärkung der Eigenverantwortung des Individuums im Sinne des Gesundheitsgesetzes beitragen. Diese Wirkung kann das EPD nur erzielen, wenn es rasch eine grosse Verbreitung findet, wenn die Funktionalitäten einer kantonsweiten Stammgemeinschaft einschliesslich eines leistungsfähigen Benutzersupports zur Verfügung stehen und wenn alle stationären und ambulanten Leistungserbringer der Behandlungskette eingebunden sind. Zudem ist der Kanton nicht nur Gewährleister der Gesundheitsversorgung, sondern auch Eigentümer und Betreiber eigener Spitäler. Er hat ein Interesse daran, dass seinen Spitälern rechtzeitig eine technische Infrastruktur für das EPD zur Verfügung steht. Der Kanton unterstützt daher den Aufbau der Infrastruktur und der Betriebsorganisation im Kanton Zürich (vgl. Antrag des Regierungsrates vom 22. Dezember 2015, Vorlage 5247, Bewilligung eines Beitrages aus dem Lotteriefonds zugunsten des Vereins Trägerschaft ZAD). Das Ausführungsrecht und insbesondere die Bestimmungen in der Verordnung über die Finanzhilfen für das elektronische Patientendossier betreffen daher die Interessen des Kantons direkt.

2. Überblick über die Vernehmlassungsdokumente

2.1 Unterlagen auf www.vernehmlassungen.zh.ch

Das Ausführungsrecht ist umfangreich und recht technisch gehalten. Es ist nicht einfach, es zu durchdringen. Es besteht aus drei Verordnungen (EPDV, EPDV-EDI, EPDFV) sowie deren Anhängen (siehe unten Ziff. 2.3 bis Ziff. 2.5).

EPDG und Ausführungsrecht regeln die Rechte und Pflichten der Patientinnen und Patienten (u.a. Vertraulichkeitsstufen und Zugriffsrechte), die Aufgaben und Pflichten der Gemeinschaften und Stammgemeinschaften (u.a. Verwaltung, Datenhaltung und -übertragung, Datenschutz und -sicherheit, Kontaktstelle, Zugangsportal), die Identifikationsmittel, die Akkreditierung und Zertifizierung, die Abfragedienste und die Finanzhilfen. Das Schreiben des EDI (Beilage) enthält als Orientierungshilfe Angaben, wo was geregelt ist. Von besonderer Relevanz ist Anhang 2 der EPDV-EDI (Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften, TOZ): In den TOZ wird eingehend geregelt, welche Anforderungen Gemeinschaften und Stammgemeinschaften zu erfüllen haben. Die TOZ sind auch für die Leistungserbringer relevant, denn indirekt enthalten sie auch die Vorgaben, die die Leistungserbringer zu erfüllen haben.

Wir haben die Vernehmlassungsunterlagen, die auf der Webseite des BAG zur Verfügung stehen, neu beschriftet und in zwei Archive gepackt (erhältlich ter www.vernehmlassungen.zh.ch):

(1) **VL_AR_EPDG_Unterlagen_Verordnungen_Anhänge_Erläuterungen.zip**: allgemeine Vernehmlassungsunterlagen sowie Gesetzestexte mit Anhängen

(2) VL_AR_EPDG_Normen_Standards_Profile_Hintergrundinformationen.zip: Normen, Standards, Profile und zusätzliche Informationen

Für die **Beantwortung der Fragen** (vgl. Ziff. 3) benötigen Sie in erster Linie **Datei (1)**. Wir haben in Ziff. 2.3 bis Ziff. 2.5 einige Punkte oder Bestimmungen herausgegriffen, die uns aufgefallen sind und die wir für diskussionswürdig halten.

2.2 Erste Einschätzung

Insgesamt halten wir das gesamte Paket für recht unübersichtlich und schwerfällig. Das EPDG selbst regelt inhaltlich fast nichts, sondern besteht mehr oder weniger aus Delegationsnormen. Zwar ist die EPDV etwas konkreter. Dennoch enthält auch sie viele Verweisungen. Näheres enthalten erst die Anhänge zur EPDV-EDI. Diese sind sehr technisch und umfangreich. Zudem verzichtet der Bund bei einem Grossteil der Anhänge auf eine Übersetzung in die Amtssprachen. Die fehlende Übersetzung halten wir insbesondere bei Anhang 8 (Vorgaben für den Schutz der Identifikationsmittel) für problematisch. Bedeutung und Inhalt dieses Anhangs erschliessen sich nur schwer.

Die TOZ (siehe Ziff. 2.4) sind einerseits sehr detailliert und teilweise ausufernd, gehen aber andererseits inhaltlich nicht wesentlich über das hinaus, was bereits in der EPDV enthalten ist. Insbesondere im Bereich Verschlüsselung und Datenablage halten wir die TOZ trotz ihrer Ausführlichkeit für lückenhaft. Es fragt sich, ob es nicht besser wäre, das Wesentliche generell-abstrakt zu formulieren und in die EPDV aufzunehmen. Unseres Erachtens wird die Aufsicht über das EPDG und seine Verordnungen in zu weit gehender Weise an (private) Zertifizierungsstellen delegiert.

Es besteht die Gefahr, dass die Umsetzung des Ausführungsrechts zu erheblichen Kosten führen wird. Insbesondere die Vorgabe, dass alle Systeme mit persistent gespeicherten Daten des EPD netzwerktechnisch von allen anderen Systemen, die ein tieferes Sicherheitsniveau aufweisen, zu separieren sind, dürfte zu erheblichem Mehraufwand führen. Das Gleiche gilt für die komplexe Struktur des EPD (vier Vertraulichkeitsstufen mit vielfältigen Möglichkeiten für die Patientinnen und Patienten, Zugriffsrechte zu vergeben und zu entziehen). Die Zwei-Faktor-Authentifizierung ist zwar grundsätzlich zu begrüssen, die Umsetzung erscheint aber als kompliziert und für die Leistungserbringer aufwendig.

Insgesamt erhalten wir den Eindruck, dass die Umsetzung des Ausführungsrechts in der Form, wie sie in die Vernehmlassung gegeben wurde, für die Kantone, die Gemeinschaften und Stammgemeinschaften und vor allem die Leistungserbringer erheblichen Aufwand verursachen dürfte. Es fragt sich, ob nicht eine Vereinfachung und Entschlackung vorgenommen könnte.

2.3 Verordnung über das elektronische Patientendossier (EPDV)

Die **EPDV** (Dateien VL_AR_EPDG_EPDV_) enthält (teilweise) das grundlegende Ausführungsrecht zum EPDG. Beispiele:

Art. 1: Vertraulichkeitsstufen

Art. 2: Zugriffsrechte

Art. 9 Abs. 1 lit. c: Daten des EPD dürfen nur in Ablagen gespeichert werden, die ausschliesslich dafür vorgesehen sind

Art. 11: Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem betreiben

Art. 11 Abs. 4: Datenspeicher müssen sich in der Schweiz befinden

Art. 22: Identifikationsmittel

Art. 23: Identitätsprüfung

Art. 27: Akkreditierung

Art. 33: Überwachung der Einhaltung der Zertifizierungsvoraussetzungen

Art. 36: Schutzklausel (Noteingriffsrechte des BAG)

Art. 38: Abfragedienste

Art. 42 Gebühren: Gemeinschaften und Stammgemeinschaften müssen eine jährliche Gebühr von Fr. 13'500 bezahlen; zusätzlich anwendbar ist die Allgemeine Gebührenverordnung des Bundes.

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

Die **EPDV-EDI** (Dateien VL_AR_EPDG_EPDV-EDI_) führt die Bestimmungen der EPDV näher aus. Relevant sind vor allem die Anhänge. Dazu gehören beispielsweise:

Anhang 2: Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (**TOZ**): Das (bereits im EPDG angelegte) System mit akkreditierten Zertifizierungsstellen hat zur Folge, dass die Anforderungen, die Gemeinschaften und Stammgemeinschaften zu erfüllen haben, erst in den TOZ eingehender geregelt werden. Es empfiehlt sich daher, die TOZ anzuschauen. Sie sind recht umfangreich. Beispielhaft seien erwähnt:

Ziff. 1.4.3.1: starkes Authentifizierungsverfahren mit Zwei-Faktor-Authentifizierung (2FA); vgl. auch Ziff. 8.3.3.1.

Ziff. 1.4.3.2: vertrauenswürdiger Endpunkt für die sichere Kommunikation mit dem Identitätsdienstleister; vgl. auch Ziff. 8.3.3.2.

Ziff. 2.6.1.2: Notfallzugriff nur nach einer nochmaligen Bestätigung mit unverzüglicher Information der Patientin (Ziff. 2.6.1.3).

Ziff. 2.9.24: Für den Datenaustausch mit der Identifikationsdatenbank der ZAS muss die Datenaustauschplattform SEDEX des Bundesamtes für Statistik verwendet werden.

Ziff. 4.2.1: Datenschutz- und Datensicherheitsmanagementsystem gemäss ISO/IEC 27001:2013.

Ziff. 4.8.1: Nur behandlungsrelevante Daten dürfen im EPD zugänglich gemacht werden.

Ziff. 4.8.2: Alle schützenswerten Daten, Systeme und Einrichtungen des EPD müssen eindeutig identifiziert, klassifiziert und in einem Inventar erfasst werden.

Ziff. 4.9.2: Endgeräte, die von Gesundheitsfachpersonen für den Zugriff auf das EPD verwendet werden, müssen sicher konfiguriert werden.

Ziff. 4.10.2.3: Gemeinschaften müssen sicherstellen, dass Personen, die Zugang zu Daten des EPD erlangen könnten, einer der ärztlichen Schweigepflicht analogen Verpflichtung unterliegen [?]; siehe auch Ziff. 5.1.2.2

Ziff. 4.10.3.1 und 4.10.3.2: Gemeinschaften müssen eine Liste aller Personen führen, die Zugriff auf Patientendaten haben („Liste der Schlüsselpersonen“) und diese Personen einer Personensicherheitsprüfung nach Militärgesetz unterziehen [?].

Ziff. 4.14.2.1: Die Produktivumgebung muss von anderen Umgebungen isoliert sein und von anderen Systemen des Betreibers mittels eigener Netzwerkzonierung isoliert sein (Ziff. 4.14.2.5).

Ziff. 4.16.1: Die Übertragung von Daten des EPD innerhalt von Gemeinschaften und zwischen Gemeinschaften muss durch geeignete und dem Stand der Technik entsprechende kryptographische Massnahmen gegen den Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden.

Ziff. 4.17.1: Besonders schützenswerte [nicht aber andere?] Daten des EPD müssen mit geeigneten kryptographischen Massnahmen verschlüsselt und integritätsgeschützt sein.

Ziff. 4.18.1.4: Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schüsseln müssen physisch geschützt werden.

Ziff. 4.19.1.2: Netzwerke müssen so verwaltet werden, dass Daten des EPD in Anwendungen und Systemen vor unautorisierten Zugriffen geschützt sind.

Ziff. 4.20.2.1: Alle Systeme mit persistent gespeicherten Daten des EPD sind netzwerktechnisch von allen anderen Systemen zu separieren, die ein tieferes Sicherheitsniveau aufweisen.

Ziff. 4.21.1 / 4.21.2: Interagiert eine Gesundheitsfachperson zwei Stunden nicht mit dem EPD, muss sie sich vor dem nächsten Zugriff erneut authentisieren.

Ziff. 6.1.4.6: Mitarbeitende des „Service-Desks“ müssen per Fernsteuerung auf die Endgeräte von Patientinnen zugreifen können [?].

Ziff. 9.1.1: Das Zugangsportal muss den einschlägigen rechtlichen Anforderungen entsprechen [?].

Anhang 4 liegt noch nicht vor. **Anhang 3** zählt die **Metadaten** auf, und **Anhang 8** enthält **Vorgaben für den Schutz von Identifikationsmitteln**. Letztere dürften sich primär an die Herausgeber solcher Mittel richten.

2.5 Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV)

Die **EPDFV** (Dateien VL_AR_EPDG_EPDFV_) regelt die **Finanzhilfen für** den **Aufbau** und die **Zertifizierung** einer Gemeinschaft oder Stammgemeinschaft. **Nicht abgedeckt** durch die Finanzhilfen des Bundes sind die Kosten für den **Betrieb**. Nur Gemeinschaften und Stammgemeinschaften können Finanzhilfen beantragen (Art. 2 Abs. 1 EPDFV). Hausarztpraxen, Spitäler und weitere Gesundheitsfachpersonen, die ihre lokalen Praxis- oder Klinikinformationssysteme an die Erfordernisse des EPD anpassen möchten, erhalten keine Finanzhilfen.

Pro Kanton können höchstens zwei Gemeinschaften oder Stammgemeinschaften unterstützt werden (Art. 1 Abs. 2 EPDFV).

Der **Höchstbetrag für Stammgemeinschaften** ist limitiert auf **Fr. 500'000** (Art. 4 Abs. 1 EPDFV). Die EPDFV behandelt die Kantone unterschiedslos. Aus Sicht des Kantons Zürich fragt sich, ob diese Regelung nicht zu starr ist. Zudem fragt sich, was geschieht, wenn eine Stammgemeinschaft für das Gebiet mehrerer Kantone Leistungen erbringt. Der Höchstbetrag wird ergänzt durch eine **variable Komponente** (Art. 5). Die für die Bemessung der Finanzhilfen **anrechenbaren Kosten** sind **im Anhang** der EPDFV aufgelistet.

Der Kanton hat zu einem Gesuch innert zwei Monaten Stellung zu nehmen (Art. 9 Abs. 2). Er muss dabei unter anderem angeben, wie hoch die durch den Kanton oder Dritte zugesicherten finanziellen Beiträge sind (Hinweis: Gemäss Art. 20 Abs. 2 EPDG werden **Finanzhilfen nur gewährt, wenn sich die Kantone oder Dritte in mindestens gleicher Höhe beteiligen**).

3. Aufforderung zu Stellungnahme / zu klärende Fragen

Das Ausführungsrecht zum EPDG sollte so ausgestaltet sein, dass die Ziele des EPDG erreicht werden können, ohne dass der Aufwand für die Umsetzung durch die Kantone und die Leistungserbringer übermässig wird.

Wir bitten Sie, zum Ausführungsrecht Stellung zu nehmen. Um uns die Abfassung der Vernehmlassungsantwort des Kantons zu erleichtern, ersuchen wir sie, dabei insbesondere folgende Fragen zu beantworten:

1. Ist das kantonale Recht mit dem Ausführungsrecht kompatibel? Besteht Anpassungsbedarf?

2. Welche finanziellen Auswirkungen hat das Ausführungsrecht auf den Kanton?

3. Lässt sich das Ausführungsrecht bei den Leistungserbringern umsetzen? Welcher Aufwand ist damit verbunden?

4. Ist das System der Finanzierungshilfen sinnvoll? Werden die Interessen des Kantons Zürich und der hier ansässigen Leistungserbringer in der EPDFV genügend berücksichtigt?

5. Berücksichtigt das Ausführungsrecht die Belange des Datenschutzes ausgewogen?

6. Ist die Struktur des Ausführungsrechts sachgerecht?

Wir bitten Sie, uns Ihre Mitberichte bis spätestens **Mittwoch, 18. Mai 2016** (eintreffend), elektronisch zuzustellen (marius.kobi@gd.zh.ch).

Gerne erwarten wir Ihre Stellungnahmen, bedanken uns im Voraus für Ihre Bemühungen, stehen für die Beantwortung von Fragen zur Verfügung und verbleiben

mit freundlichen Grüssen.

Marius Kobi

Beilage: Schreiben EDI vom 22. März 2016: Eröffnung Anhörung Ausführungsrecht EPDG

Verteiler:
– Direktionen des Regierungsrates und Staatskanzlei
– Datenschutzbeauftragter des Kantons Zürich
– Stadt Zürich, Gesundheits- und Umweltdepartement
– USZ, KSW
– PUK, ipw
– VZK, Curaviva Kanton Zürich
– Ärztegesellschaft des Kantons Zürich, Spitex-Verband Zürich, Apothekerverband des Kantons Zürich