Einschreiben
Bundesamt für Gesundheit
Abteilung Multisektorale Projekte
3003 Bern

Bern, den 20. Dezember 2011

Vernehmlassung: Neues Bundesgesetz über das elektronische Patientendossier - Stellungnahme

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, im Rahmen der Vernehmlassung für das neue Bundesgesetz über das elektronische Patientendossier Stellung nehmen zu können.

1. Vorbemerkungen

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 900 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.

ISSS wurde 1993 als Verein unter dem früheren Namen FGSec gegründet. ISSS ist Mitglied von ICTswitzerland und offizieller Security Fachpartner von SwissICT.

Unsere Stellungnahme beschränkt sich auf diejenigen Punkte des Gesetzesentwurfes, welche im Zusammenhang mit der ICT-Sicherheit und dem Informationsschutz stehen.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anträge.

2. Allgemein

Gesundheitsdaten sind besonders sensible Daten und stellen speziell hohe Anforderungen an die Wahrung der Vertraulichkeit und die Sicherstellung von Richtigkeit und Unverfälschtheit. Rechtlich hat dies seinen Niederschlag insbesondere in der beruflichen Schweigepflicht für Medizinalpersonen, in der Strafnorm zur Verletzung des Arztgeheimnisses von Art. 321 StGB sowie im Datenschutzrecht gefunden, wo Gesundheitsdaten als besonders schützenswerte Daten gelten, für die erhöhte Schutzanforderungen gelten. In der kantonalen Gesundheitsgesetzgebung finden sich sodann im Zusammenhang mit dem Einsatz der elektronischen Behandlungsdokumentation spezifische Anforderungen betreffend Authentizität, Integrität, Revisionsfähigkeit (Nachverfolgbarkeit) und Verfügbarkeit der Daten bzw. Systeme.

Das ePatientendossier ist als ein Abrufverfahren für dezentral gespeicherte Patientendaten zwischen verschiedenen Organisationen im Gesundheitswesen konzipiert. Damit ist das Risiko verbunden, dass die Daten nicht autorisierten Personen zu Kenntnis gelangen oder dass die Daten unbefugterweise oder aufgrund technischer Fehler verfälscht oder vernichtet werden. Das ePatientendossier ist jedoch zwingend auf das Vertrauen der betroffenen Personen, das heisst in erster Linie der Patienten, aber auch der Gesundheitsfachpersonen, angewiesen. Ohne dieses Vertrauen der Betroffenen wird das ePatientendossier sich nicht durchsetzen können.

Der ICT-Sicherheit und dem Datenschutz kommen daher für den Erfolg des ePatientendossiers entscheidende Bedeutung zu. Dies gilt umso mehr, als die Nutzung des ePatientendossiers sowohl für die Patienten als auch für die Gesundheitsfachpersonen (ausgenommen Spitäler im Sinn von Art. 18 der Schlussbestimmungen des Gesetzesentwurfs) freiwillig ist.

3. Art. 1: Gegenstand des Gesetzes – Verankerung der ICT-Sicherheit und des Informationsschutzes

Trotz der zentralen Bedeutung, welche der ICT-Sicherheit und dem Datenschutz für das ePatientendossier zukommt, werden diese im Grundsatzartikel von Art. 1 des Entwurfs nicht erwähnt. Dies ist unseres Erachtens jedoch notwendig, um sicherzustellen, dass diesen Aspekten im Rahmen der konkretisierenden Regelungen, welche in weiten Bereichen der Verordnungsgebung überlassenen sind, stets das erforderliche Gewicht eingeräumt wird.

Gerade im Hinblick darauf, dass aus Gründen der Praktikabilität ein erheblicher Druck besteht, möglichst einfach handhabbare Lösungen vorzusehen, was in einem Zielkonflikt zur Sicherheit stehen kann, ist klarzustellen, dass der Sicherheitsaspekt nicht vernachlässigt werden darf. Andernfalls besteht die Gefahr, dass zwar eine einfach zu nutzende Lösung gewählt wird, die jedoch wegen der ungenügenden Sicherheit von den betroffenen Personen abgelehnt bzw. nicht genutzt wird.

Antrag:

Art. 1 Abs. 3 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„[2] Mit dem elektronischen Patientendossier …… gesteigert werden. ***Dem Datenschutz und der Datensicherheit ist stets in angemessener Weise Rechnung zu tragen.***“

4. Art. 2: Definitionen – Ergänzung der „Stammgemeinschaft“

Lediglich aus dem erläuternden Bericht geht hervor, dass der Stammgemeinschaft, das heisst derjenigen zertifizierten Gemeinschaft, welche initial das ePatientendossier für einen Patienten erstellt, eine zentrale Funktion im System des ePatientendossier zukommt. Die Stammgemeinschaft ist zuständig für die Entgegennahme und Aufbewahrung der Einwilligungserklärung zur Errichtung des ePatientendossiers sowie eines allfälligen Widerrufs. Bei der Stammgemeinschaft werden ferner die Zugriffsrechte hinterlegt. Im Hinblick auf diese zentrale Rolle der Stammgemeinschaft und die damit verbundene Verantwortlichkeit ist es notwendig, diese im Gesetz zu verankern.

Antrag:

Art. 2 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„……

„***e. Stammgemeinschaft: zertifizierte Gemeinschaft, welche für eine Patientin oder einen Patienten das ePatientendossier einrichtet und bestimmte für dessen Betrieb wesentliche Funktionen wahrnimmt.“***

5. Art. 3: Einwilligung des Patienten – Notwendige Präzisierungen

5.1 Einwilligung zur Erstellung eines Patientendossiers an die „Stammgemeinschaft“

Gemäss Art. 3 Abs. 1 des Entwurfs muss der Patient seine schriftliche Zustimmung zur Erstellung eines elektronischen Patientendossiers erteilen.

Da es sich beim ePatientendossier um ein virtuelles Dossier handelt, bei dem die Daten dezentral von den verschiedenen Gemeinschaften verwaltet und gespeichert werden, bei welchen sich ein Patient in Behandlung befindet, ist es nicht selbstverständlich, gegenüber wem ein Patient die Grundsatzeinwilligung zur Einrichtung des elektronischen Patientendossiers zu erklären hat. Aus dem Erläuterungsbericht ergibt sich, dass diese Erklärung gegenüber irgendeiner der zertifizierten Gemeinschaften, welche am ePatientendossier teilnimmt und bei der sich der Patient in Behandlung befindet, erfolgen kann. Diese Gemeinschaft gilt dann gemäss Erläuterungsbericht als „Stammgemeinschaft“. Sie richtet in der Folge das ePatientendossier für den Patienten ein, bewahrt die Einwilligungserklärung zu Beweiszwecken auf und erfüllt weitere Funktionen im Zusammenhang mit dem elektronischen Patientendossier.

Dies findet im Gesetzestext jedoch keinen Niederschlag. Insbesondere im Hinblick auf die rechtliche Relevanz der Einwilligungserklärung und den Umstand, dass diese Erklärung nicht nur für die Stammgemeinschaft, sondern auch für alle anderen Gemeinschaften, welche in der Folge Daten in das ePatientendossier einstellen oder von dort abrufen, von grundlegender Bedeutung ist, ist die Zuständigkeit für die Entgegennahme und Aufbewahrung der Einwilligungserklärung klarzustellen. Ebenso ist zu regeln, wie lange die Einwilligungserklärung aufzubewahren ist.

Antrag:

Art. 3 Abs. 1 des Gesetzesentwurfs sei wie folgt zu modifizieren (fetter und kursiver bzw. durchgestrichener Text):

„[1] Die Patientin oder der Patient muss ***gegenüber der Stammgemeinschaft*** schriftlich einwilligen, dass ein elektronisches Patientendossier erstellt wird. ***Die Einwilligungserklärung ist von der Stammgemeinschaft während einer Frist von mindestens zehn Jahren nach Auflösung des elektronischen Patientendossiers aufzubewahren.***“

5.2 Einwilligung zum Zugänglichmachen von Daten

In Übereinstimmung mit den Grundsätzen des Datenschutzes wird gemäss Abs. 2 von Art. 3 des Entwurfes für das Zugänglichmachen von Daten eines Patienten dessen ausdrückliche Einwilligung verlangt. Die Formulierung dieser Bestimmung ist dahingehend unklar, als offen ist, worauf sich die Einwilligung beziehen muss.

Im Rahmen der Diskussionen um den Gesetzesentwurf wurden hierzu unterschiedliche Auffassungen geäussert, was zeigt, dass Klärungsbedarf besteht. Eine Auffassung geht dahin, dass eine einmalige und generelle Einwilligung des Patienten genügt, wonach die ihn behandelnden Gesundheitsfachpersonen Daten in sein elektronisches Patientendossier einstellen dürfen. Diese Auffassung ist zu weitgehend. Die Einwilligung betreffend das Zugänglichmachen der Daten würde gewissermassen mit der Einwilligung zur Erstellung eines Patientendossiers verbunden und hätte damit keine selbständige Bedeutung. Es könnte damit auf Art. 3 Abs. 2 des Entwurfs verzichtet werden.

Das entgegengesetzte Extrem stellt die Auffassung dar, dass die Einwilligung für jedes einzelne Dokument notwendig sei. Dies dürfte aus Gründen der Praktikabilität nicht realisierbar sein.

Dem Patienten muss jedoch das Recht zustehen, die Einstellung bestimmter Dokumente in das ePatientendossier zu untersagen, wie er auch ausserhalb des ePatientendossiers die Möglichkeit hat, anzuordnen, dass bestimmte Daten nicht an Dritte (vor- oder nachbehandelnde Ärzte, Therapeuten etc.) weitergegeben werden dürfen.

Eine weitere Lösung besteht darin, dass die Einwilligung jeweils gegenüber einer einzelnen Gemeinschaft erteilt wird, und diese in der Folge alle bei ihr über den betreffenden Patienten anfallenden behandlungsrelevanten Daten in das elektronische Patientendossier einstellen darf (und gemäss Art. 6 des Entwurfs auch muss). Auch dies ist aus datenschutzrechtlicher Sicht zu weitgehend. Auch ausserhalb des ePatientendossiers bezieht sich die datenschutzrechtliche Patientenerklärung jeweils nicht generell auf die Bearbeitung sämtlicher Daten, welche im Lauf der Zeit anfallen, sondern gilt jeweils mit Bezug auf die Daten im Zusammenhang mit einer bestimmten Behandlung. Dies allein scheint mit den geltenden Datenschutzgrundsätzen vereinbar und entspricht auch den in der Praxis bereits eingespielten Abläufen betreffend Patienteninformation und Patienteneinwilligung.

Antrag:

Art. 3 Abs. 2 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„[2] Sie oder er muss ausdrücklich einwilligen, dass die eigenen***, im Zusammenhang mit einer bestimmten Behandlung stehenden*** Daten zugänglich gemacht werden. ***Sie oder er kann bestimmen, dass bestimmte Daten nicht zugänglich gemacht werden dürfen.***“

5.3 Widerruf der Einwilligung

Die Regelung in Art. 3 Abs. 4 des Entwurfs ist dahingehend unklar, als nicht ersichtlich ist, ob sich der Widerruf nur auf eine der in Abs. 1 und 2 erwähnten Einwilligungen bezieht, und falls ja, auf welche, oder ob Abs. 4 den Widerruf beider Arten von Einwilligung regelt.

Nach den Grundsätzen des Datenschutzes muss der Widerruf für beide Einwilligungen möglich sein. Auch der erläuternde Bericht (S. 43) geht davon aus, dass der Widerruf gemäss Abs. 4 für die Einwilligung sowohl gemäss Abs. 1 als auch gemäss Abs. 2 möglich ist.

a) Notwendige Präzisierung der Modalitäten

Gemäss dem erläuternden Bericht (S. 43) soll der Widerruf dadurch erfolgen, dass die Zugriffsrechte gelöscht werden. Die Einrichtung und Löschung von Zugriffsrechten durch den Patienten wird jedoch in Art. 4 des Entwurfs geregelt. Eine besondere Vorschrift betreffend den Widerruf wäre gar nicht notwendig, wenn dieser nur im Entzug der Zugriffsrechte bestehen würde.

Ebenso ist unter dieser Voraussetzung nicht nachvollziehbar, warum die „Stammgemeinschaft“ eine Widerrufserklärung verwalten müsste, wie im erläuternden Bericht (S. 43) ausgeführt. Eine solche Erklärung wäre gar nicht notwendig, wenn der Widerruf mit der Löschung der Zugriffsrechte durch den Patienten gleichzusetzen wäre.

Anders verhält es sich hingegen, wenn die mit dem Widerruf verbundene Aufhebung der Zugriffsrechte nicht durch den Patienten gemäss Art. 4 des Entwurfs selbst vorgenommen würde, sondern durch seine „Stammgemeinschaft“, gegenüber welcher er den Widerruf erklärt. Dann würde es Sinn machen, dass diese die Widerrufserklärung aufzubewahren hätte. Der Entwurf regelt jedoch diese Möglichkeit der Löschung von Zugriffsrechten durch die Stammgemeinschaft nicht, was jedoch notwendig ist, wenn diese Möglichkeit tatsächlich gegeben sein soll (vgl. dazu unten Ziff. 8).

Nicht nachvollziehbar ist zudem, warum im erläuternden Bericht im Zusammenhang mit dem Widerruf nur die Stammgemeinschaft erwähnt wird. Die Widerrufserklärung gegenüber der Stammgemeinschaft ist nachvollziehbar, wenn es sich um Daten handelt, welche von der Stammgemeinschaft in das ePatientendossier eingestellt wurden oder wenn die Einwilligung zum ePatientendossier als solche widerrufen werden soll. Falls der Widerruf sich jedoch auf Daten bezieht, welche von einer anderen Gemeinschaft als der Stammgemeinschaft ins ePatientendossier eingestellt wurden, muss dieser gegenüber der betreffenden Gemeinschaft erklärt werden.

Im Übrigen erscheint es sinnvoll, für den Widerruf des ePatientendossiers als solchem (wie für die Zustimmung zu diesem gemäss Abs. 1 von Art. 3) Schriftlichkeit zu verlangen, während für den Widerruf einzelner Dokumente die Nachweisbarkeit unabhängig der Form genügt.

b) Notwendige Präzisierung der Folgen

Gemäss dem erläuternden Bericht hat der Widerruf zur Folge, dass die Zugriffsrechte entzogen werden. Damit besteht jedoch das widerrufene ePatientendossier fort und Daten, für welche der Widerruf erklärt wurde, verbleiben weiterhin in dem Online-Abrufsystem. Dies entspricht jedoch nicht dem, was man allgemein von einem Widerruf erwarten würde, nämlich, dass die im ePatientendossier enthaltenen Daten insgesamt (bei Widerruf des Dossiers als solchem gemäss Art. 3 Abs. 1) oder zum Teil (beim Widerruf der Einwilligung zur Einstellung bestimmter Daten gemäss Art. 3 Abs. 2) gelöscht oder zumindest aus dem Kontext des Online-Abrufsystems entfernt werden, das heisst, die entsprechenden Indizierungen aufgehoben werden und in einen vom aktiven Online-System separierten Archivbereich überführt werden.

Aus Sicht der Datensicherheit und des Datenschutzes wäre es bedenklich, dass das ePatientendossier bzw. die darin enthaltenen Daten, für welche der Patient den Widerruf erklärt hat, weiterhin im System verbleiben und lediglich keine aktuellen Zugriffsrechte mehr bestehen. Damit bleiben widerrufene ePatientendossiers bzw. Daten den mit dem System verbundenen Risiken ausgesetzt, z.B. dem unautorisierten Zugriff auf die Daten durch Missbrauch der Identifikationsmittel des Patienten. Ein Grund, warum ein Patient den Widerruf erklärt, dürfte jedoch gerade darin liegen, diese Risiken auszuschliessen.

Die weitere Bewahrung des ePatientendossiers bzw. der Daten, für welche der Widerruf erklärt wurde, lässt sich auch nicht mit der gesetzlichen Pflicht zur Führung der Behandlungsdokumentation rechfertigen. Das ePatientendossier dient ja lediglich dem Abruf von Daten, nicht der Erfüllung der Dokumentationspflicht.

c) Antrag

Antrag:

Art. 3 Abs. 4 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„[4] Die Patientin oder der Patient kann die Einwilligung ***gemäss Abs. 1 oder Abs. 2*** widerrufen. ***Der Widerruf ist gegenüber der Stammgemeinschaft bezüglich der Einwilligung gemäss Abs. 1 schriftlich und bezüglich der Einwilligung gemäss Abs. 2 nachweisbar gegenüber derjenigen Gemeinschaft, welche die betreffenden Daten in das elektronische Patientendossier eingestellt hat, zu erklären. Die vom Widerruf betroffenen Daten der Patientin oder des Patienten sind aus dem elektronischen Patientendossier zu entfernen bzw. dieses ist aufzulösen.***“

6. Art. 4: Zugriffsrechte – Klärung der Möglichkeiten des Patienten

6.1 Möglichkeit zur Löschung von Daten

Nach Art. 4 Abs. 1 lit. a des Entwurfs hat der Patient die Möglichkeit, auf die eigenen Daten zuzugreifen. Diese Zugriffsmöglichkeit ist um die weitere Möglichkeit zu ergänzen, Daten aus dem Patientendossier zu entfernen. Da die Weitergabe von Patientendaten von der Zustimmung des Patienten abhängig ist und dessen Einwilligung bedarf, muss der Patient auch einzelne Daten bzw. Dokumente aus dem ePatientendossier entfernen können. Es kann insoweit auf die Bemerkungen oben in Ziff. 5.3 betreffend die Wirkungen des Widerrufs verwiesen werden.

Mit Rücksicht darauf, dass die Gesundheitsfachpersonen die Verantwortung für die inhaltliche Richtigkeit der Daten bzw. Dokumente tragen, ist dem Patienten jedoch keine Berechtigung einzuräumen, die von den Gemeinschaften in das elektronische Patientendossier eingestellten Daten zu modifizieren. Dagegen wäre die Möglichkeit der Annotation der Daten durch den Patienten in Form von klar als vom Patienten stammenden Kommentaren durchaus sinnvoll.

Antrag:

Art. 4 Abs. 1 lit. a des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

…….
„

a. über ein zertifiziertes Zugangsportal auf die eigenen Daten zugreifen, diese annotieren ***und diese aus dem elektronischen Patientendossier entfernen***."

6.2 Einsehbarkeit der Protokollierung für Patienten

Sämtliche Zugriffe auf Dokumente im Rahmen des ePatientendossiers sind zu protokollieren (vgl. Entwurf Art. 8 Abs. 1 lit. d). Gemäss dem erläuternden Bericht (S. 49f.) hat der Patient das Recht auf jederzeitige Einsicht in die Protokolldaten. Dieses Recht muss jedoch in Form eines entsprechenden Gesuchs an die jeweilige Gemeinschaft ausgeübt werden. Dies stellt eine erhebliche Schwelle zur Rechtsausübung dar. Es ist daher vorzuziehen, wenn die Patienten zusätzlich die Möglichkeit haben, über das Zugangsportal die Protokollierungen über die erfolgten Zugriffe auf ihre Daten jederzeit ohne weitere Hürden einzusehen.

Antrag:

Art. 4 Abs. 1 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„……
e. den Zugriff von Gesundheitsfachpersonen in medizinischen Notfallsituationen ausschliessen.
f. Einsicht in die Protokollierungen der Zugriffe auf ihre/seine Daten nehmen.“

6.3 Stellvertretung

Aus dem Gesetzesentwurf wird nicht klar, wie die Zugriffsverwaltung für Patienten erfolgt, welche nicht in der Lage sind, diese selber vorzunehmen (dauernd oder vorübergehend handlungsunfähige Personen). Eine Lösung besteht darin, dass die Verwaltung der Zugriffsrechte auch durch die Stammgemeinschaft eines Patienten erfolgen kann, die sich hierfür wiederum auf die allgemeine Stellvertretungsregelung abstützt, wie sie sich aus dem Zivilrecht und der Gesundheitsgesetzgebung ergeben. Allerdings ist im Entwurf nirgends vorgesehen, dass eine Stammgemeinschaft diese Funktion erfüllen kann und darf.

Eine weitere Möglichkeit wäre, dass innerhalb des Berechtigungssystems von einem Patient anderen zugriffsberechtigten Personen, seien es Gesundheitsfachpersonen oder Patienten, die Berechtigung erteilt werden kann, stellvertretungsweise für einen Patienten die in Art. 4 des Entwurfes vorgesehenen Möglichkeiten (Datenzugriff und Rechteverwaltung) vorzunehmen. Diese Stellvertretungsberechtigung wäre als ein besonderer Berechtigungstyp innerhalb des Systems auszugestalten. Eine solche Stellvertretungsregelung ist aus praktischer Sicht wünschbar.

Antrag:

Art. 4 Abs. 1 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„……
e. den Zugriff von Gesundheitsfachpersonen in medizinischen Notfallsituationen ausschliessen.
f. ……[vgl. oben Ziff. 6.2]
g. einzelnen Patientinnen oder Patienten oder Gesundheitsfachpersonen die Berechtigung einräumen und entziehen, die Möglichkeiten gemäss lit. a-f stellvertretungsweise für die Patientin oder den Patienten wahrzunehmen.“

7. Art. 5: Identifikation

7.1 Sichere elektronische Identität

Der Begriff der sicheren elektronischen Identität ist inhaltlich nicht eindeutig.

Die genaue Festlegung der Identifikationsmittel und der Anforderungen an den Ausgabeprozess erfolgt gemäss Abs. 4 von Art. 5 des Entwurfs auf Verordnungsebene, was sinnvoll ist. Wesentlich ist dabei jedoch, dass auch hier die Mitwirkung sichergestellt ist (dazu unten zu Art. 10) und dass der Datensicherheit und dem Datenschutz das notwendige Gewicht beigemessen wird (vgl. oben Ziff. 3).

Für die Sicherheit des elektronischen Patientendossiers ist nicht nur die sichere elektronische Identität wichtig, sondern auch, dass eine sichere Authentisierung sichergestellt ist. In Abs. 4 von Art. 5 ist daher zu ergänzen, dass der Bundesrat auf Verordnungsebene auch bezüglich der Authentisierung entsprechende Mindestanforderungen festlegt.

Antrag:

Art. 5 Abs. 4 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„Er legt die zugelassenen Identifikationsmittel und die Anforderungen an deren Ausgabeprozess ***sowie Mindestanforderungen betreffend einer starken (Zweifaktor-)Authentisierung*** fest."

8. Art. 6: Pflicht der Gemeinschaften – Notwendige Ergänzungen, insbesondere betreffend die Schlüsselfunktion der „Stammgemeinschaft"

Die Stammgemeinschaft eines Patienten spielt eine bedeutende Rolle im Zusammenhang mit der Einwilligung des Patienten zum ePatientendossier sowie einem allfälligen Widerruf.

Aus dem Bericht (S. 45) sowie den Empfehlungen III ergibt sich, dass der Stammgemeinschaft noch weitere Aufgaben, insbesondere im Zusammenhang mit der Verwaltung der Zugriffsrechte, zukommen. Diese werden in den Empfehlungen III (S. 22) wie folgt umschrieben:

Eine Stammgemeinschaft kann auf Anfrage einer zertifizierten Gemeinschaft

- *angeben, dass sie die Stammgemeinschaft zu einem bestimmten Patienten ist;*
- *angeben, welche Einwilligungen und Zugriffsrechte (inklusive Black List) zu einem Patienten bestehen;*
- *Einwilligungen und Zugriffsrechte zu[sic.!] verändern;*
- *die Eigenschaft „Stammgemeinschaft" einer Person an eine andere Gemeinschaft weitergeben (z.B. im Falle eines Umzugs).*

Wie bereits erwähnt sind die Stammgemeinschaft und ihre Funktionen aus dem Gesetzesentwurf nicht ersichtlich. Im Hinblick darauf, dass die Stammgemeinschaft für den Patienten wesentliche Aufgaben erfüllt, ist es jedoch notwendig, diese Rolle im Gesetz klar zu verankern.

Dies im Hinblick einerseits auf die rechtliche Verantwortlichkeit, welche der Stammgemeinschaft im Verhältnis zu den Patienten bezüglich der Wahrung des Datenschutzes und der Datensicherheit zukommt, und andererseits mit Rücksicht darauf, dass eine klare Regelung der Verantwortlichkeit der Stammgemeinschaft im Zusammenhang mit allfälligen Haftungsfällen zentral ist.

Sofern der Stammgemeinschaft die Funktion zukommt, anstelle des Patienten Zugriffsrechte einzuräumen oder zu ändern (und dies vom Patienten nicht ausschliesslich allein über das Zugangsportal gemacht wird, was nicht realistisch erscheint), muss dies im Sinn einer Verpflichtung der Stammgemeinschaft gesetzlich verankert werden. Das gilt insbesondere, wenn eine Änderung von Zugriffsrechten und Einwilligungen auf „Anfrage einer anderen Gemeinschaft" erfolgt. Dies kann ohne die Zustimmung des Patienten nicht in Frage kommen, denn es ist der Patient, der über die Zugriffsberechtigungen entscheidet und ebenso über seine Einwilligung bzw. einen allfälligen Widerruf. Denkbar ist allerdings, dass ein Patient die Stammgemeinschaft im Voraus zur Vornahme bestimmter Änderungen ermächtigt. Als standardmässiger Stellvertreter des Patienten könnte automatisch die erste Stammgemeinschaft, welche Daten im Patientendossier ablegt, gewählt werden.

Auch eine Weitergabe der Funktion als Stammgemeinschaft kann mit Rücksicht auf die wichtige Rolle, welche die Stammgemeinschaft für den Patienten und die Wahrung von dessen informationeller Selbstbestimmung erfüllt, nur mit Zustimmung des Patienten erfolgen, und nicht auf blossen Antrag einer anderen Gemeinschaft.

Bezüglich der Ergänzung in Abs. 1 betreffend den Widerruf kann auf das oben in Ziff. 5.3 lit. b Gesagte verwiesen werden. Zusätzlich ist die Pflicht zu Protokollierung ausdrücklich festzuhalten, welche in der aktuellen Fassung des Entwurfs lediglich aus Art. 8 Abs. 1 lit. d abgeleitet werden kann. Die Protokollierungspflicht ist jedoch für das System von zentraler Bedeutung und daher explizit festzuhalten, so dass dem Patienten ein direkter Anspruch gegenüber den Gemeinschaften entsteht.

Ebenso ist klarzustellen, dass die Protokolle vom Auskunftsanspruch des Patienten erfasst sind.

Schliesslich ist die Archivierung der aus dem elektronischen Patientendossier entfernten Dokumente sowie der Protokolle zu regeln.

Im Gesetz ist auch festzulegen, dass das elektronische Patientendossier nach dem Tod eines Patienten aufzuheben ist und die darin enthaltenen Daten in die Archivierung überführt werden. Im Falle eines ungeklärten Todesfalls ist das Dossier bis zum Abschluss eines allfälligen gerichtlichen Verfahrens aufzubewahren.

Antrag:

Art. 6 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„***1*** Zertifizierte Gemeinschaften müssen sicherstellen, dass

a. diejenigen behandlungsrelevanten Daten über das elektronische Patientendossier zugänglich gemacht werden, zu denen die Patientin oder der Patient nach Artikel 3 Abs. 2 eingewilligt hat;

b. diese Daten, soweit sie von einem Widerruf betroffen sind, oder im Fall des Todes der Patientin oder des Patienten aus dem elektronischen Patientendossier entfernt werden, sofern ein natürlicher Tod eingetreten ist oder ein allfälliges gerichtliches Verfahren zur Feststellung der Todesursache abgeschlossen wurde;

c. die aus dem elektronischen Patientendossier entfernten Daten sicher, solange zusammen mit der genauen Zeitangabe der Einstellung in das und der Entfernung aus dem elektronischen Patientendossier sicher aufbewahrt werden, bis die Frist zur Aufbewahrung der Behandlungsdokumentation für die betreffende Patientin oder den betreffenden Patienten abgelaufen ist;

d. sämtliche Zugriffe auf die von der Gemeinschaft in das elektronische Patientendossier eingestellten Daten protokolliert und die Protokolle während der gleichen Dauer wie die Daten gemäss lit. c aufbewahrt werden.

2 Die Stammgemeinschaft einer Patientin oder eines Patienten ist verpflichtet,

a. sicherzustellen, dass die von der Patientin oder dem Patienten erteilten Zugriffsrechte bei der Stammgemeinschaft hinterlegt werden;

b. aufgrund einer von der Patientin oder dem Patienten erteilten Einwilligung im Einzelfall oder einer generellen Ermächtigung Zugriffsrechte einzuräumen, zu ändern oder aufzuheben;

c. im Fall des Widerrufs eines elektronischen Patientendossiers oder im Fall des Todes einer Patientin oder eines Patienten die anderen Gemeinschaften, die Daten im elektronischen Patientendossier zugänglich gemacht haben, über den Widerruf oder den Tod zu informieren;

d. die Funktion der Stammgemeinschaft nach Anweisung der Patientin oder des Patienten auf eine andere zertifizierte Gemeinschaft zu übertragen.“

9. Art. 7 Zertifizierungspflicht – Zertifizierungsmöglichkeit für Dienstleister

Es ist davon auszugehen, dass für viele Gesundheitsfachpersonen und Gemeinschaften die für die Teilnahme am ePatientendossier erforderliche Zertifizierung mit einem erheblichen internen Aufwand sowie beträchtliche externen Kosten verbunden sein wird, welche unter Umständen prohibitiv wirken könnten. Die Möglichkeit, dass sich einzelne oder Organisationen von Gesundheitsfachpersonen zu Gemeinschaften zusammenschliessen können, um einheitlich eine Zertifizierung für die gesamte Gemeinschaft zu erlangen, stellt deshalb einen Weg dar, um den Aufwand für die einzelne Gesundheitsfachperson/Organisation in Grenzen zu halten.

Zusätzlich ist jedoch zu prüfen, ob nicht auch die weitere Möglichkeit vorzusehen ist, dass sich im Gesundheitssektor tätige Anbieter von IT-Dienstleistungen, die für Gesundheitsfachpersonen oder Organisationen Systeme betreiben, welche im Zusammenhang mit dem ePatientendossier eingesetzt werden, z.B. Outsourcing- und ASP-Anbieter, sich ebenfalls sollten zertifizieren lassen können. Dies würde dann für eine einzelne Gesundheitsfachperson bzw. Organisation, welche die Dienstleistungen eines zertifizierten Anbieters in Anspruch nimmt, bedeuten, dass nur noch derjenige Aufwand und diejenigen Kosten zur Zertifizierung von Systemen und Prozessen anfallen, soweit diese sich im Bereich der betreffenden Gesundheitsfachperson bzw. Organisation befinden.

Antrag:

Art. 7 des Gesetzesentwurfs sei wie folgt um einen neuen Abs. 2 zu ergänzen (fetter und kursiver Text):

„[1] Für die Bearbeitung ……

„[2] Anbieter, die Informatik-Dienstleistungen an Gemeinschaften erbringen, können sich zertifizieren lassen.“

10. Art. 10: Mitwirkung – Umfang der Mitwirkung

Nach Art. 10 Abs. 2 stellt der Bund bei der Vorbereitung rechtsetzender Erlasse nach den Artikeln 8 und 9 die Mitwirkung der Kantone und Anhörung der betroffenen Organisationen auf geeignete Weise sicher. Dies ist unter zwei Aspekten zu erweitern:

1. Die Mitwirkung ist nicht nur auf die unmittelbar durch das ePatientendossier betroffenen Organisationen zu beschränken, sondern es sind auch weitere Organisationen einzubeziehen, welche aufgrund ihrer Ziele einen Bezug zu den durch das ePatientendossier betroffenen Themen haben, z.B. die ISSS, insoweit es sich um Fragen der ICT-Sicherheit handelt.

2. In die Mitwirkung sind zudem auch die Vorbereitung rechtsetzender Erlasse nach Art. 5 des Entwurfs (Bestimmung der Identifikationsmerkmale sowie Festlegung der Identifikationsmittel und Anforderungen an die Ausgabeprozesse; dazu bereits oben Ziff. 7.1) sowie die Festlegung der technischen Anforderungen betreffend Verzeichnisse, Abfragedienste und den nationalen Kontaktpunkt gemäss Abs. 3 von Art. 11 einzubeziehen. Das gleiche gilt auch für Ausführungsbestimmungen, welche gestützt auf die generelle Verordnungskompetenz des Bundesrats erlassen werden, z.B. zur näheren Ausführung der Definitionen in Art. 2 des Gesetzes.

Antrag:

Art. 10 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„Der Bund stellt bei der Vorbereitung …… Erlassen, ***insbesondere*** nach den Artikeln **5**, 8 und 9 ***sowie bei der Festlegung von technischen Anforderungen nach Artikel 11 Abs. 3,*** die Mitwirkung der Kantone sowie die Anhörung der betroffenen ***oder interessierten*** Organisationen sicher."

11. Art. 12: Information – Benutzerschulung für die Patienten

Nach Abs. 3 von Art. 3 des Entwurfes muss es sich bei der Einwilligung gemäss den Absätzen 2 und 3 um einen „Informed Consent" handeln, das heisst, der Patienten muss über Art und Umfang der Datenbearbeitung, zu welcher er einwilligt, deren möglichen Folgen und die damit verbundenen Risiken hinreichend informiert sein.

Aufgrund der Komplexität des Systems und der grossen Eigenverantwortung, welche dem Patienten insbesondere für die Vergabe und Verwaltung von Zugriffsrechten zukommt, dürfte es nicht genügen, wie dies heute sonst im Zusammenhang mit der Information der Patienten über die Bearbeitung ihrer Daten üblich und auch ausreichend ist, den Patienten ein blosses Merkblatt abzugeben. Die Patienten benötigen vielmehr eine weitergehende Erläuterung, Erklärung und Schulung betreffend die ihnen im Rahmen des ePatientendossier zur Verfügung stehenden Möglichkeiten. Sind die Patienten nicht in der Lage, von diesen Möglichkeiten korrekt Gebrauch zu machen, ist einerseits die bestimmungsgemässe Nutzung in Frage gestellt, weil Gesundheitsfachpersonen, welche Zugriff haben müssten, die erforderlichen Rechte nicht erteilt sind, und andererseits entstehen Risiken für den Datenschutz und die Datensicherheit, weil falsch eingerichtete oder überholte Zugriffsrechte den Zugriff unbefugter Personen ermöglichen.

Es ist nicht realistisch anzunehmen, dass die erforderliche Information und Schulung der Patienten allein durch die behandelnden Gesundheitsfachpersonen (insbesondere in der Stammgemeinschaft) wird geleistet werden können. Dies nicht nur wegen des erforderlichen Zeitaufwandes, welcher durch die Behandelnden kaum wird erbracht werden können, sondern weil es fraglich ist, ob die Patienten überhaupt in der Behandlungssituation zu einer solchen Schulung bereit sein werden.

Es wird daher im Rahmen der Informationstätigkeit gemäss Art. 12 des Entwurfs die Information der Patienten ein zentrales Element sein müssen, was durch eine entsprechende Ergänzung des Wortlauts festzuhalten ist.

Antrag:

Art. 12 des Gesetzesentwurfs sei wie folgt zu ergänzen (fetter und kursiver Text):

„[1] Der Bund …… über das elektronische Patientendossier. ***Er sorgt für eine hinreichende Information der Patientinnen und Patienten betreffend die Ausübung der ihnen nach Art. 4 zur Verfügung stehenden Möglichkeiten.***“

Mit freundlichen Grüssen

Dr. Thomas Dübendorfer
Präsident ISSS

Dr. Ursula Widmer
Vizepräsidentin ISSS

Ich habe dieses Dokument bestätigt
Qualifiziert signiert durch Thomas Dübendorfer
Information Security Society Switzerland
Zürich, 14. Dezember 2011

Information Security Society Switzerland (ISSS)
Wasserwerkgasse 37
3000 Bern 13

E-Mail: Dr. Thomas Dübendorfer: president@isss.ch
E-Mail: Dr. Ursula Widmer: vicepresident@isss.ch