Stellungnahme zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, Gesetzentwurf vom 22.6.2015

Drucksache 18/5293

Dr. André Zilch (Sachverständiger und Fachexperte Identitätsmanagement CertEuropA GmbH, Geschäftsführer LSc LifeScience Consult GmbH, Geschäftsführer ValiPic (Deutschland) GmbH)

Die CertEuropA GmbH ist eine bundesweit tätige, akkreditierte Zertifizierungsstelle sowie anerkannte fachkundige Stelle für Qualitätsmanagementsysteme und Angebote zum Identitätsmanagement. Die LSc LifeScience Consult GmbH ist fokussiert auf die Analyse und Gestaltung datenschutzkonformer Geschäftsprozesse nach nationalen und internationalen Standards für das Identitätsmanagement und insbesondere die Gestaltung von registrier- und identitätsbetätigenden Verfahren unter Berücksichtigung des öffentlichen und privaten Rechts sowie der Wettbewerbskonformität. Die ValiPic (Deutschland) GmbH ist ein Anbieter zur Durchführung datenschutzkonformer registrier- und identitätsbestätigender Verfahren insbesondere für den Banken- und Gesundheitsbereich.

Vorbemerkung:

Mehr als 10 Jahre nach Verabschiedung des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung, mit dem die Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur (TI) verabschiedet wurde, muss festgestellt werden, dass bisher keines der gesetzlich verankerten Ziele zeitgerecht und/oder inhaltlich erreicht werden konnte.

Trotz zunehmender Einflussnahme durch das Bundesministerium für Gesundheit, begleitet von ergänzenden gesetzlichen Vorgaben und Verordnungen, konnte die Gesamtleistung der Gematik zur Einführung der TI nicht verbessert werden.

Neben den komplexen technischen Aufgaben war und ist die Gematik auch mit organisatorischen Aufgaben betreut. So gilt es, unterschiedlichste Rechtsgebiete und internationale Vorschriften und Normen zu berücksichtigen und in technischen und organisatorischen Spezifikation abzubilden. Dies hat in Kombination mit dem durch die lange Laufzeit des Gesamtprojektes bedingten technischen Fortschritt und der Mitarbeiterfluktuation in der Gematik zu einer erheblichen Zunahme der Komplexität geführt. Die technische, organisatorische und rechtliche Komplexität hat im Ergebnis zu teilweise gravierenden Mängeln in der Umsetzung geführt, soweit sie denn überhaupt erfolgt ist.

Deutscher Bundestag
Ausschuss f. Gesundheit

Ausschussdrucksache
18(14)0139(24)
gel. ESV zur öAnhörung am 04.11.
15_eHealth
02.11.2015

Im Einzelnen:

Mit dem vorliegenden Gesetzentwurf sollen Maßnahmen etabliert werden, die im Wesentlichen durch eine verbindliche Vorgabe von Fristen die Einführung der TI sicherstellen soll. Gleichzeitig sollen aber auch der Gematik neue Aufgabengebiete übertragen werden, ohne jedoch zunächst z.B. die Pflichtanwendung „e-Rezept", die in der Gesetzesbegründung aus 2003 als wesentliche Anwendung bestimmt wurde, umzusetzen.

Alle aktuell geplanten Anwendungen wie Medikationsplan oder Notfalldaten sind freiwillige Anwendungen. Es derzeit nicht abzuschätzen, inwieweit Versicherte diese Angebote nutzen werden, da gerade an der organisatorischen Schnittstelle, nämlich der Arzt-Patienten Beziehung, keine Überzeugung pro TI auf Seiten der Ärzteschaft zu erkennen ist.

Der von Kritikern bezweifelten Kosten-Nutzen Relation kann nicht wirksam begegnet werden, wenn die freiwilligen Anwendungen nicht von der Mehrzahl der Versicherten genutzt werden. Dies gilt umso mehr, als sich am Markt durch den Glaubwürdigkeitsverlust der Aussagen zur Einführung der TI Alternativen und Parallelstrukturen entwickeln bzw. entwickelt haben, die einer freiwilligen Nutzung durch Versicherte entgegenwirken.

Der vorliegende Gesetzentwurf lässt jedoch keine grundsätzliche Beseitigung der strukturellen Ursachen der Probleme zur Einführung der TI erkennen.

Als strukturelle Ursache ist zunächst die Gestaltung der Gematik als GmbH zu nennen und zu hinterfragen, da die Gesellschafterstruktur immer wieder als Grund für zeitverzögerte Entscheidungen genannt wird.

- Mit Einführung der Schlichterstelle wurde in den vergangenen Jahren auch der Einfluss des BMG wesentlich gestärkt, ohne dass jedoch echte Fortschritte im Ergebnis zu erkennen sind.
- Der vorliegende Gesetzentwurf erweitert das Aufgabenspektrum um die Tätigkeiten zum Aufbau eines Interoperabilitätsverzeichnisses.
- Die Existenz von Parallelnetzen ist zwar zunächst möglich, jedoch sollen mit Bereitstellung der TI diese Netze integriert oder obsolet werden.
- Das Aufgabenfeld und die Einnahmen der Gematik sind nicht durch privatwirtschaftliche Tätigkeiten geprägt.
- Der vorliegende Gesetzentwurf führt darüber hinaus Gebührentatbestände sowie die Festlegungen zur Bestimmung der Höhe der Gebühren ein.

In Summe sprechen diese Umstände für überwiegend nicht-privatwirtschaftlich geprägte Tätigkeiten der Gematik.

Daher sollte der Gesetzgeber prüfen, inwieweit eine Umwandlung der Gematik in eine Körperschaft des öffentlichen Rechts oder eine Behörde eine Zielerreichung zur Einführung der TI wahrscheinlicher werden lässt und dem objektiven Handeln der Gematik besser gerecht wird.

Die im Gesetzentwurf vorgeschlagenen Pönalen bei Nichterreichung festgesetzter Fristen für einzelne Gesellschafter der Gematik dürften als nicht vereinbar mit dem GmbH-Gesetz einzuordnen sein.

Mit hoher Priorität sollte eine Reduzierung der Komplexität angestrebt werden. Um Erfolge bei der Einführung der TI erfolgreich vorantreiben zu können, sollten die bestehenden Aufgaben der Gematik reduziert und priorisiert sowie veröffentlichte Zeitpläne eingehalten werden.

Das LSG NRW hat festgestellt, dass ein Ruhen des Leistungsanspruchs auf der eGK entsprechend den gesetzlichen Regelungen zwar gespeichert werden „kann", aber nicht „muss". Weiterhin haben Krankenhäuser keinen Anspruch auf Vorlage einer eGK und können aus der Vorlage der eGK keinen „Versicherungsnachweis" ableiten, so wie im aktuellen Änderungsvorschlag zu §291 geplant ist. Die aktuellen Regelungen zur Vorgehensweise bei Nichtvorlage der eGK im BMV-Ä dürften rechtlich unwirksam sein. Die Vorgehensweise bei Nichtvorlage der eGK sollte der Gesetzgebern in §15 (2) SGB V regeln.

Nicht mehr der gelebten Praxis entsprechende Regelungen werden jedoch nicht aufgegeben. So bestätigt kaum ein Versicherter bei Inanspruchnahme ärztlicher Behandlung auf dem Abrechnungsschein des Arztes das Bestehen der Mitgliedschaft durch seine Unterschrift (s. §291 Abs. 1 Satz 5 SGB V).

Offensichtliche Regelungslücken in der bisherigen Gesetzgebung, die teilweise durch Gerichte bereits erkannt wurden, werden nicht beseitigt.

Zwar wird auch im vorliegenden Gesetzentwurf dem Datenschutz höchste Priorität eingeräumt, jedoch lassen die beschriebenen rechtlichen und technischen Maßnahmen die unabdingbar notwendigen organisatorischen Maßnahmen oder rechtliche Klarstellungen vermissen. Ohne diese organisatorischen Maßnahmen und rechtlichen Klarstellungen wird jedoch der Datenschutz ad absurdum geführt. Was nutzt der vielbeschriebene sichere Zugangsschlüssel eGK zur TI, wenn nicht sichergestellt ist, dass auch nur derjenige den Schlüssel nutzen kann, der durch die Angaben der Zertifikate und der optischen Merkmale wie Lichtbild und Unterschrift auch tatsächlich beschrieben ist?

Neben den genannten strukturellen Ursachen für das bisherige Scheitern der Einführung der TI ist auch der ungenügend umgesetzte Datenschutz bei der Einführung der elektronischen Gesundheitskarte wesentlich für den Glaubwürdigkeitsverlust in der Öffentlichkeit.

Das BSI fordert in der entsprechenden Richtlinie „Elektronische Identitäten und Vertrauensdienste im E-Government" basierend auf dem korrespondierenden internationalen ISO Standard ein vertrauenswürdiges Identitätsmanagement, welches die Basis für alle weiteren Aktivitäten ist:

- Die Identitätsprüfung muss mindestens auf dem Vertrauensniveau des Authentisierungssystems erfolgen, für das das Enrolment durchgeführt wird.

- Die Identitätsprüfung muss auf der Basis amtlicher Dokumente/Register erfolgen, wobei die Zugehörigkeit der Dokumente/der Registereinträge zur Entität (Anm. Person) sichergestellt werden muss, etwa durch einen sicheren Lichtbildvergleich.

Dies ist auch im Sicherheitskonzept der Gematik reflektiert, welches für den Rollout der eGKs verbindlich ist.

Um die gesetzlichen und datenschutzrechtlichen Anforderungen an einen Identitätsnachweis im Gesundheitswesen zu erfüllen, müssen neben den etablierten technischen Voraussetzungen wie z.B. Zertifikate, Verschlüsselungsalgorithmen und PIN-Länge auch die organisatorischen Voraussetzungen erfüllt sein.

Bei den Beantragungs-/Ausgabeverfahren der eGK muss eine Bestätigung der Identität und der Adresse durch eine vom Benutzer unabhängige Instanz erfolgen, die ihrerseits dem Vertrauensniveau der zu schützenden Daten genügen muss. Werden jedoch (Teil-)Verfahren eingesetzt, die den notwendigen Schutzbedarf nicht erfüllen, so werden alle weiteren Sicherheitsmechanismen kompromittiert.

Selbstbestätigungen durch Versicherte sowie Datenübernahme aus Ausweisdokumenten von Arbeitgebern im Rahmen von DEÜV-Verfahren erfüllen diese Anforderungen nicht und alle weiteren Sicherheitsmechanismen müssen als kompromittiert angesehen werden.

Damit können z.B. VSD, Notfalldaten oder Organspendeerklärungen mit aktuell ausgegebenen eGKs nicht datenschutzgerecht umgesetzt werden.

Wie sollten Informationen des Notfalldatensatzes genutzt werden können, wenn nicht sichergestellt ist, dass diese Daten auch der zu behandelnden Person zuzuordnen sind? So wird in der unter Mitwirkung des BMG von BearingPoint und Fraunhofer Fokus durchgeführten Planungsstudie zur Interoperabilität als Hemmnis für Notfalldatensätze ausgeführt: „Sicherstellung, dass Datenträger (Notfallausweis, eGK, etc.) tatsächlich der zu behandelnden Person zuzuordnen ist."

Zentraler Punkt zur Sicherstellung des Datenschutzes ist die rechtliche Klarstellung der eGK als Identitäts- und Versicherungsnachweis in §291 SGB V.

Der Gesetzgeber hat am 28.6.12 in seinem Beschluss zu Petition 5298 bereits bestätigt, dass die eGK Identitätsnachweis ist.

Dies gilt sowohl für die eGK als visueller Identitätsnachweis (aufgedruckte administrative Daten wie Lichtbild) als auch als elektronischer Identitätsnachweis (Zertifikate).

In §36a SGB I wurde bestimmt, dass die eGK in der Kommunikation zwischen Versicherten und Krankenkassen als elektronischer Identitätsnachweis gleichberechtigt zur eID Funktion eingesetzt werden kann.

Dies ist auch folgerichtig, denn in Artikel 1, Nummer 10 Buchstabe b, Doppelbuchstabe b heißt es, dass die eGK Zitat:„die Durchführung der Anwendungen nach §291a Absatz 2 und 3 zu gewährleisten hat."

Weiterhin heißt es in der Gesetzesbegründung zu §36a SGB I in Bt-Drs. 17/11473: „Abweichend von der Änderung des § 3a VwVfG wird in Satz 5 2. Halbsatz für die Kommunikation zwischen dem Versicherten und seiner Krankenkasse die elektronische Gesundheitskarte als möglicher weiterer elektronischer Nachweis der Identität zugelassen."

Um diese Forderungen des Gesetzgebers erfüllen zu können, ist es aber zwingend notwendig, dass die eGK auch die Identität des Versicherten zweifelsfrei nachweist und sich alle Teilnehmer an der Telematik sicher sein können, dass Person und Karte zusammengehören. Das ist durch die gesetzliche Verankerung der eGK als Identitätsnachweis sichergestellt.

Aber: Die Krankenkassen erfüllen die verbindlichen Anforderungen nicht, die sich für die Beantragung und Ausgabe ergeben. Das verwundert auch nicht, denn für den Spitzenverbands der Krankenkassen ist die eGK nur ein eingeschränkter Identitätsnachweis.

Einen „eingeschränkter Identitätsnachweis" gibt es jedoch nicht und diese Aussage steht im Widerspruch zur Gesetzesbegründung zu §36a SGB I.

Was würde diese Einschränkung umfassen? Zu 80% das Geburtsdatum, den Vornamen oder den Namen? Oder würde nur die Adresse gelten und nicht der Name?

Um auf Sozialdaten zugreifen zu können, ist der Nachweis der Identität Grundvoraussetzung, d.h., dass die eGK zur Authentisierung geeignet sein muss, so auch der Gesetzgeber in §291 Abs. 2a Satz 4.

Authentisierung ist definiert als der Nachweis von behaupteten Eigenschaften. Diese sind hier einerseits der Nachweis der Identität des Versicherten (bei der die eGK vorlegenden Person handelt es sich tatsächlich um die Person, die durch die eGK beschrieben ist) und andererseits der Versicherungsnachweis.

Um Rechtssicherheit zu garantieren, muss die eGK dementsprechend nicht nur als Versicherungsnachweis sondern auch als Identitätsnachweis in der Überschrift zu §291 formuliert werden.

Die aktuellen Verfahren der Krankenkassen zur Ausgabe der eGK erfüllen die genannten nationalen und internationalen Vorschriften nicht, obwohl bereits 2004 im Rahmen von b4health die Architekturentscheidung getroffen wurde, die Beantragungs- und Ausgabeverfahren auf das Sicherheitsniveau der eGK anzupassen. Das ist sowohl dem BMG als auch den Spitzenverbänden der Krankenkassen seit dieser Zeit bekannt.

Trotzdem werden entgegen der Absicht des Gesetzgebers und dem Sicherheitskonzept der Gematik die Gesundheitskarten mit dem für Identitätsnachweise zwingend notwendigen Beantragungs- und Ausgabeverfahren ausgegeben. Deshalb dürfen die ausgegebenen eGKs nicht für Anwendungen nach §291a eingesetzt werden. Daran ändern auch die geplanten PINs nichts, da immer noch die sichere Zuordnung zum Versicherten durch eine bestätigende Stelle fehlt.

Aktuell haben Ärzte keine Möglichkeit, unbefugte Zugriffe im Rahmen des VSD datenschutzgerecht zu unterbinden.

Alle Regelungen des vorliegenden Gesetzentwurfs zur Nutzung eines PINs gehen vollständig fehl, solange die eGK nicht entlang eines vorgegebenen Verfahrens entsprechend der Schutzbedarfsklasse für Sozialdaten ausgegeben werden - nur dann kann die eGK als vollwertiger Identitätsnachweis genutzt werden.

Es geht also nicht nur darum, dass die eGK „Versicherungsnachweis" ist, sondern auch, dass der Versicherte seine Identität gegenüber allen Leistungserbringern und der Telematikinfrastruktur verbindlich nachweist.

Zusammenfassend lässt sich zur eGK als Identitäts- und Versicherungsnachweis folgendes feststellen:

Die vorgeschlagene Klarstellung des §291 mit der Bezeichnung „Identitäts- und Versicherungsnachweis" ist unabdingbar.

Sollten die bisherigen Verfahren zur Beantragung/Ausgabe der eGKs nicht geändert werden, darf kein Zugriff auf Sozialdaten erfolgen.

Aktuell sind alle eGKs grundsätzlich nicht für Anwendungen nach §291a einsetzbar, d.h. weder VSD noch Notfalldaten können rechtssicher genutzt werden.

Entweder die eGK ist Identitätsnachweis, dann darf sie als Zugangsmittel zu Sozialdaten (z.B. Notfalldaten, VSD) genutzt werden, oder sie ist kein Identitätsnachweis, dann kann sie nicht datenschutzgerecht als Authentisierungsinstrument für Sozialdaten genutzt werden.

Sollten die nicht als Identitätsnachweis nutzbaren eGKs dennoch eingesetzt werden, könnte dies den Straftatbestand nach §203 StGB für diejenigen erfüllen, die mittels eGK Sozialdaten offenbaren z.B. VSD, Notfalldaten. Zudem es könnte ein Verstoß gegen EU-Regelungen vorliegen.

Damit wären alle unmittelbaren und zukünftigen Ziele einer Telematikinfrastruktur und des e-health Gesetzes nicht erreichbar und es würde keine datenschutzgerechte Telematik in Deutschland geben.

Eppstein, den 2. November 2015