LD7.1

Tel.: 988-1208
17.04.2008

LD 17.04.2008

PIN-Management bei der elektronischen Gesundheitskarte (eGK)

Im Rahmen der Testung der eGK in Flensburg hat sich gezeigt, dass viele, ja oft die Mehrzahl der PatientInnen, insbesondere ältere, besonders kranke und behinderte Menschen, Probleme mit der PIN ihrer eGK haben. Viele können sich an sie nicht erinnern. Manche sind auch nicht in der Lage, die PIN auf der Tastatur – in der geforderten Zeit – einzutippen. Die Forderung der im Projekt beteiligten ÄrztInnen geht dahin, auf die PIN zu verzichten bzw., da eine Autorisierung per PIN gesetzlich und technisch vorgesehen ist, die PIN in diesen Fällen einheitlich auf 000000 (sog. Default-PIN) zu stellen.

Es besteht in Schleswig-Holstein Einigkeit, dass der Umstand, dass wegen der o.g. Umstände die betroffenen Personen von der Nutzung der EGK nicht ausgeschlossen können und dürfen. Es besteht ebenso Einigkeit, dass eine praktikable Lösung gefunden werden muss, bei der sowohl die gesetzlichen Vorgaben als die materiellen Ziele zur Wahrung des Datenschutzes berücksichtigt bleiben.

Die Nutzung einer Default-PIN würde das Ziel, die Sicherung der Daten doppelt (durch Wissen und Besitz) zu gewährleisten, untergraben. Zwar würde formell der Anforderung der Eingabe einer PIN genügt, doch würde dabei vollständig das Schutzziel ignorieren. Der Umstand, dass die Betroffenen hierin einwilligen, genügt nicht als Kompensation, da diese Einwilligung i.d.R. nicht freiwillig sein dürfte: Will und muss eine Person die Karte nutzen, kann aber die PIN nicht handhaben, so ist sie gezwungen, in die Default-PIN einzuwilligen.

Das Risiko einer Default-PIN ist aus Datenschutzsicht auch nicht hinnehmbar: Bei den betroffenen Personen dürfte es sich regelmäßig um solche handeln, über die eine Vielzahl hochsensibler medizinischer Informationen per eGK erschlossen werden. Würde die Karte verloren, was gerade bei der betroffenen Personengruppe immer wieder passieren kann, so genügt irgendeine Health Professional Card, um an die sensiblen Daten zu gelangen. Dass an diesen Daten Dritte (z.B. Versicherungen, Arbeitgeber) auch ein großes Interesse haben können, ist unbestreitbar. Es käme einer nicht zu rechtfertigenden Diskriminierung von Menschen gleich, wenn diese wegen ihrer Behinderung gezwungen wären, auf die übliche angemessene technische Datensicherung zu verzichten.

Es stellt sich daher die Frage, welche Maßnahmen ergriffen werden können, mit denen eine vergleichbare Sicherheit erreicht werden kann wie durch die PIN-Eingabe durch den Betroffenen. Denkbar sind zunächst Alternativen, die an die Stelle des Wissens einen anderen Berechtigungsnachweis erbringen, etwa biometrische Verfahren. Diese dürfte aber zum derzeitigen Projektstand kurzfristig nicht zu realisieren sein.

Denkbar sind aus meiner Sicht auch Alternativen, die jeweils auf einem Treuhändermodell basieren, d.h. dass eine andere Person/andere Personen/eine bestimmte Stelle für den Patienten die PIN kennt, zur Verfügung stellen kann und eingibt. In jedem Fall bedarf die Beauftragung zur treuhänderischen Verwaltung der PIN (PIN-Management) einer Vollmacht, die z.B. in Schriftform erteilt werden kann. In jedem Fall muss für die genannten Fälle das PIN-Management vorab festgelegt und eindeutig für alle Betroffenen beschrieben sein. Spontanlösung (z.B. Schreiben der PIN auf die Karte) genügen den Sicherheitsanforderungen nicht.

Als Treuhänder kommt zunächst der behandelnde Arzt in Betracht. Dieser kann die PIN in der Patientenakte (elektronisch oder konventionell) dokumentieren. Hier genießt sie den gleichen Schutz wie die sonstigen dort gespeicherten Daten (Patientengeheimnis). Zugleich wird die Patientenakte regelmäßig ohnehin geöffnet sein, wenn die eGK zum Einsatz kommt. Im Fall einer Überweisung kann die PIN wie sonstige sensiblen medizinischen Informationen an den weiterbehandelnden Arzt weitergegeben werden. Im Notfall denkbar ist sogar die telefonische Weitergabe der PIN an einen anderen Arzt, wenn die Berechtigung des anfordernden Arztes und dessen Authentizierung hinreichend gesichert sind und die PIN-Weitergabe in der Akte hinreichend dokumentiert wird. Insofern unterscheidet sich die Weitergabe nicht von sonstigen medizinisch notwendigen Spontanübermittlungen.

Die Beauftragung des behandelnden Arztes als Treuhänder muss sich nicht auf den Hausarzt beschränken. In Grunde kann jeder behandelnde Arzt nach einem vorgegebenen Verfahren mit dem PIN-Management beauftragt werden. Mit dem beschriebenen Verfahren lässt sich eine – wohl nicht so oft vorkommende – Fallkonstellation nicht bewältigen: Der Patient kommt zu einem neuen Arzt und die trauhänderisch beauftragten Ärzte sind nicht sofort erreichbar.

Denkbar ist in diesen Fällen die zusätzliche Beauftragung einer (möglichst zentralen) Stelle, die rund um die Uhr erreichbar ist. Diese müsste die PINs sowie einige weitere Daten (z.B. beauftragte Ärzte, Angaben, weshalb PIN vom Patienten nicht genutzt werden kann) verwalten und im Bedarfsfall auf Nachfrage herausgeben. Durch geeignete Maßnahmen muss Autorisierung und Authentizierung des anfragenden Arztes geklärt werden.

Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz