Beitrag von RD Dipl. Inf. Walter Ernestus, Referat VI der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für Sommerakademie 2015 „Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutzziel“

eGK und Telematik-Infrastruktur – eine Baustelle für sensibelste Datenverarbeitung

Die Einführung der elektronischen Gesundheitskarte zieht sich jetzt schon fast 10-Jahre hin. Im 5. Buch des Sozialgesetzbuches (SGB) im § 291a Abs. 1 wird die Einführung bis spätestens 1.Jan. 2006 angekündigt. Doch im Feld ist die Karte noch lange nicht. Erst 2015 wurde mit der flächendeckenden Einführung der Karte begonnen. Allerdings alles nur OFFLINE, quasi als Ersatz für die (dumme) alte Krankenversichertenkarte, deren Technologie schon längst der Karten-Steinzeit zu zurechnen ist. OFFLINE bedeutet auch, dass ein wesentlicher Vorteil der elektronischen Gesundheitskarte nicht genutzt werden kann. Medizinische Anwendungen zum Nutzen des Versicherten. Im Abs. 2 und 3 von § 291a sind die Anwendungen genannt die mit der Karte verwirklicht werden soll:

„(2) Die elektronische Gesundheitskarte hat die Angaben nach § 291 Abs. 2 zu enthalten und muss geeignet sein, Angaben aufzunehmen für

1. die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form (**elektronisches Rezept**) sowie
2. den Berechtigungsnachweis zur Inanspruchnahme von Leistungen in einem Mitgliedstaat der Europäischen Union, einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz. § 6c des Bundesdatenschutzgesetzes findet Anwendung.

(3) Über Absatz 2 hinaus muss die Gesundheitskarte geeignet sein, folgende Anwendungen zu unterstützen, insbesondere das Erheben, Verarbeiten und Nutzen von

1. medizinischen Daten, soweit sie für die Notfallversorgung erforderlich sind, (**NFD)**

2. Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation (**elektronischer Arztbrief**),

3. Daten zur Prüfung der Arzneimitteltherapiesicherheit, (**AMTS**)
4. Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (**ePA)**
5. durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten, (**Patientenfach**)
6. Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten (§ 305 Abs. 2), (**Patientenquittung)**
7. Erklärungen der Versicherten zur Organ- und Gewebespende, (**OSA)**
8. Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende sowie
9. Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen nach § 1901a des Bürgerlichen Gesetzbuchs;

Diese Regelungen wurden in der Vergangenheit wiederholt verändert und ergänzt. Auf rechtlichen Betrachtungen dieser Regelung möchte ich in diesem Vortrag verzichten. Im Folgenden soll es vielmehr darum gehen, welche technischen Probleme aus den Regelungen erwachsen und welche derzeit noch nicht abschließend gelöst sind.

Das PIN-Problem

Der Zugriff auf die med. Daten des Versicherten und den sensiblen administrativen Daten ist im Gesetz klar geregelt (§ 291a Abs. 5 SGB V). Dort wird der Zugriff auf die Daten an das Vorhandensein einer Autorisierung des Versicherten und an einen Heilberufeausweis bzw. an eine Signaturkarte geknüpft. Diese Regelung hat sich über die Jahre etwas geändert und den technischen Möglichkeiten angepasst. Die früheren Chipkarten-Betriebssystem boten die Einrichtung einer PIN-Autorisierung.

Durch die Eingabe der PIN-CH konnte die eGK freigeschaltet werden. Der Arzt, ausgewiesen durch einen HBA, hätte dann Zugriff auf alle Daten nehmen können. Eine wiederholte Freigabe durch die Eingabe einer PIN wäre nicht erforderlich gewesen. Diese Vorgehensweise erfüllte nicht die datenschutzrechtlichen Anforderungen, da die Eingabe der PIN-CH alle Anwendungen freischaltete. Die Datenhoheit des Versicherten war in Gefahr. Die konsequente Weiterentwicklung des Kartenbetriebssystems hat dieses Dilemma beseitigt. Nunmehr ist es möglich nehmen der Freischaltung der eGK, beispielsweise zum Lesen von sensiblen administrativen Daten, auch jede einzelne Anwendung durch eine PIN zu schützen. Erst durch die Eingabe der Anwendungs-PIN würde dann die Anwendung (APP) dem Arzt zur Verfügung stehen. Betrachtet man dieses Verfahren genauer, stellt man zunächst zwar fest, dass hier datenschutzrechtliche Anforderungen korrekt umgesetzt werden. Gleichzeitig steigt aber die Anzahl der PIN-Eingaben ins kaum erträgliche. Die Umsetzung aller Anwendungen würde zur Folge haben, dass ein Versicherter sich bis zu 8 PIN's merken muss (PIN-CH und 7 Anwendungen). Nicht nur die Zahl der PIN schockiert, auch die Tatsache das bei allen Aktionen immer wieder der Versicherte eine PIN ins Geräte eintippen muss, geht m.E. an der Lebenswirklichkeit vorbei. Andere Lösungen wie „abschaltbare PIN", „Hinterlegen der PIN beim Arzt" wurden zwar diskutiert aber eben wieder aus IT-Sicherheitsgründen und Haftungsgründen verworfen. Die Diskussion nicht leider nicht zu Ende diskutiert, weil eine praktikable Lösung derzeit nicht in Sicht ist. Gleichwohl wird die Diskussion dann wieder aufleben, wenn die Karte ONLINE geht, also irgendwann im Jahre 2016. Hier muss eine Lösung gefunden werden die folgende Eckpunkte unter einen Hut bringt: IT-Sicherheit, Datenschutz, Praxistauglichkeit und technische Entwicklung. Forderungen nach 8 PIN beim Arzt führen nur zu heftigen Schlagzeilen in der Boulevard-Presse und demontieren die eGK als solches.

Baustelle: Bestandsnetze

Die eGK wurde zwar 2015 an alle Versicherten ausgegeben. Ihre Funktionalität beschränkt sich derzeit aber auf einen reinen KVK –Ersatz. Erst 2016 wird in Testgebieten die Integration der Karte in die Telematik-Infrastruktur vollzogen. Die Karte geht ONLINE. Dieser Schritt lenkt den Blick auf eine weitere Baustelle. Die ONLINE-Schaltung. Die Integration des Einsatzes eines Konnektors. Der Konnektor

stellt den „Sicherheitsanker“ der Telematik-Infrastruktur bei den Leistungserbringern dar (Praxen, Krankenhäusern) und soll verhindern das Unbefugte auf die Daten der Versicherten zugreifen können. Der Konnektor kontrolliert und analysiert den gesamten Datenverkehr in die TI und zum Leistungserbringer. Im Prinzip kennt der Konnektor die Fachanwendungen und würde ungesicherte Datenverkehre ablehnen. Er stellt damit einen maßgeblichen Teil der Sicherheitsinfrastruktur der TI dar. Warum wird dies dann zum Problem? Viele Arztpraxen sind heute schon ONLINE. Es werden über diese Anschlüsse verschiedene Netze betrieben und Daten getauscht. Beispielsweise KV-Safenet oder das DALE Netz. Die Anbindung solcher Praxen mit der TI hat nun die Folge das entweder diese Netze in separaten Praxis-Teilnetzen betrieben werden müssen, oder in die TI integriert werden müssen, um ein gleichbleibendes Sicherheitsniveau aufrechterhalten zu können. Andere Vorschläge beispielsweise die Einführung eines „transparenten Kanals“ im Konnektor tragen leider nicht dazu bei. Der „transparente Kanal“ im Konnektor soll den entsprechenden Datenverkehr ungehindert passieren lassen und die Sicherheit in das Benehmen der Netzbetreiber leben. Ein Lösung die eigentlich für Sicherheitsexperten nicht hinnehmbar ist. Als Zwischenlösung, quasi als Übergangslösung bis die Integration der Fachnetze in die TI vollzogen wurde, vielleicht hinnehmbar. Auf längere Sicht leider keine Option. Wer unterschiedliche Netze neben der TI betreiben will, muss in einem Sicherheitskonzept nachweisen, dass die Praxen in diesen Fällen unbefugte Zugriffe auf die med. Daten der Versicherten ausschließen können. Eine Netztrennung beim Leistungserbringer wäre unumgänglich. Doch welcher Leistungserbringer würde diese Investition schon auf sich nehmen. Eine Lösung dieses Problems steht noch aus. Aus Datenschutzsicht und aus Sicht der IT-Sicherheit muss langfristig die Integration aller med. Netze in die TI erfolgen.

Baustelle: Wahrnehmung der Versichertenrechte

Grundsätzlich soll der Versicherte die Datenhoheit über seine Daten haben. Er soll seine Daten lesen, speichern, verbergen aber auch löschen können. Das Problem das aus dieser Forderung erwächst, ist folgendes: Wie soll dies geschehen. Muss ein Versicherter, um seine Rechte wahrnehmen zu können, dies in der Nähe eines Arztes oder Apothekers tun (räumliche Nähe) oder kann dies unabhängig ohne Arzt erfolgen. Das 2 Karten Zugriffsmodell – eGK und HBA – bedingt zunächst das immer

ein HBA in der Nähe sein muss, wenn er auf seine med. Daten zugreifen will. Nur im Falle des Zugriffes auf die administrativen Daten und Protokolldaten ist dies nicht erforderlich. Für diesen Fall hat der Versicherte auch eine eigene Pin die PIN@Home. Diese ermöglicht auch den Zugriff am häuslichen PC. Die räumliche Nähe des Arztes soll dem Versicherten die Möglichkeit geben den Arzt als Vertrauensperson für die Beratung hinzuziehen. Dies aber über dieses Modell die Datenhoheit noch sichergestellt? Es gibt nur eine Ausnahme hinsichtlich dem vorhanden sein des HBA: das Patientenfach. Dort kann auch ein Zugriff ohne HBA erfolgen, es muss aber eine Signaturkarte des Versicherten zur Verfügung stehen. Wie dann der Zugriff erfolgt ist zwar immer noch nicht klar entschieden, aber die Vorgaben des §291 a wären erfüllt. Problemtisch ist beispielsweise die Frage wie stellt die eGK fest, dass die vorhandene Signaturkarte dem Besitzer der eGk gehört. Ein Konzeptpapier gibt es hierzu noch nicht. Es gibt Eckpunkte ohne konkrete Beschreibungen.
Ebenso gibt es derzeit nur sehr vage Vorstellungen wie der Versicherte beispielsweise in der Arztpraxis seine Rechte wahrnehmen kann. Das Modell eines eHealth-Kiosks macht hier die Runde. Man stellt sich dabei eine Art Bankterminal in der Arztpraxis oder Apotheke vor, an dem der Versicherte zunächst unabhängig vom Arzt seine Rechte wahrnehmen kann. Ein HBA wäre ja in der Nähe. Dort könnten auch Ausdrucke, Kopien etc. gefertigt werden. Nur wer bezahlt solche Terminals. Ein Geschäftsmodell hierzu gibt es nicht. Weder Leistungserbringer noch Kassen sehen derzeit Ihre Aufgabe im Bereitstellen eines solchen Gerätes, zumal damit erhebliche Kosten verbunden sind und eventuell auch haftungs- und Sicherheitsfragen. Auch hier stehen seit längerem die Anforderungen fest, die Umsetzung steckt allerdings noch in sehr groben Kinderschuhen. Zu befürchten bleibt, dass es nie eines solches Terminal geben wird. Es dient nur dem Datenschutz und hat keine Sicherheitsfunktion, deshalb wird von keiner Seite hier besonders darauf gedrängt solche Geräte zu entwickeln.
Wie oben bereits erwähnt gilt das Gleiche für das Patientenfach: Eckpunkte existieren zwar, ein Konzept liegt leider noch nicht.

Noch nicht aktuelle Baustelle(n)

Alle Baustellen hier aufzuführen, dazu reicht die Zeit noch. Perspektiv seinen hier aber noch einige genannt:

Berufsregister:
Zugriff nur mit Berufsausweis (HBA), bei verkammerten Berufen kein Problem, nur was ist mit allen anderen? Sperrung von Berufsausweisen ?
Einbeziehung aller Leistungserbringer in die TI ? Ist diese gewünscht? Wenn nein, was machen wir mit den Medienbrüchen?

Zuletzt bleibt noch eine Frage offen: Welche Speicherfristen von med. gespeicherten verschlüsselten Daten des Versicherten akzeptieren wir. Wer über ein Leben med. Daten beispielsweise in einer EPA gespeichert und der Versicherte stirbt kommt niemand mehr an diese Daten heran. Wer löscht diese Daten (Verschlüsselt heute sicher aber morgen?). Auch diese Frage wartet noch auf einen Lösung.

Fazit, Fragen und Anforderungen

- **Solange eGk OFFLINE ist, gibt es keine Probleme**
- **2016 geht die eGk online (VSD und NFD), spätestens dann müssen die Baustellen angegangen / beendet werden.**
- **IT-Sicherheit und Datenschutz ist nicht immer unter einen Hut zu bringen Was passiert dann?**
- **Keine datenschutzrechtlichen Forderungen bitte, die an der Lebenswirklichkeit vorbei gehen**
- **Datenschutzlücken können den „Erfolg“ der eGk gefährden (siehe Organspende)**
- **Jede Fachanwendung wird bei der gematik von dem jeweiligen Nutzer betreut (NFD => Ärzte, VSD => Kassen) Und die Rechte des Versicherten? Beispiel eHealth-Kiosk?**
- **Die Beteiligung der Versicherten und die Wahrnehmung deren Rechte ist im Falle der eGk eher unterentwickelt!**
- **Die Nutzung der eGk hängt sehr stark vom Vertrauen ab, Transparenz und Sicherheit ab. Hier gibt es Defizite!**
- **Unklar ist derzeit, wie die schnelle technologische Entwicklung im Projekt integriert werden kann Beispiel. Biometrie und PIN Problem**

- **Die Heranführung der Versicherten an die eGk findet nicht statt, weder Kassen, noch Ärzte und selbst der „Datenschutz“ hat bisher hierzu wenig geleistet.**
- **Hat sich das Konzept der „Karte“ überholt? 2006-2015/ 2016 ? Technik/Gesellschaft/Kosten?**
- **Wie gestalten wir die Prozesse der Zukunft ohne Medienbrüche?**

Walter Ernestus
--
Referat VI – BfDI -
- Verbindungsbüro Berlin -
Friedrichstr. 50-55
10117 Berlin
Email: walter.ernestus@bfdi.bund.de
Tel.: 030 187799 611