UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD • Postfach 71 16 • 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200
Aktenzeichen:
LD -71.03/01.008

Bundesbeauftragter für den Datenschutz
Landesbeauftragte für den Datenschutz

- gemäß Verteiler -

vorab per Fax

Kiel, 4. März 2005

Architekturentscheidungen zur elektronischen Gesundheitskarte (eGK)
E-Mail des BfD vom 28.02.2004, Az. IV-400-4/009#0202

Sehr geeh[redacted]
sehr geehrte Kolleginnen und Kollegen,

vielen Dank für die Zusendung der aktuellen Unterlagen zur eGK.

Bezug nehmend auf das Protokoll der Sitzung des Arbeitskreises Gesundheit und Soziales am 23./24.02.2004 in München teile ich Ihnen mit, dass durch das ULD eine Begleitung des Projektes „Gesundheitskarte Schleswig-Holstein" durch laufende Kontakte mit den für das Projekt zuständigen Personen erfolgt. Für die anderen Landesbeauftragten relevante Unterlagen wurden jeweils rundgesandt. Aus meiner Sicht macht es keinen Sinn, sämtliche im ULD auflaufenden **Unterlagen** Ihnen zur Verfügung zu stellen. Vielmehr erfolgt dies gezielt im Hinblick auf die Notwendigkeit gemeinsamer Meinungsbildung.

Ich habe die Hoffnung, dass wir Ihnen in Kürze eine Bewertung des ULD zu dem schleswig-holsteinischen Konzept des **elektronischen Rezepts** zur Verfügung stellen können. Aktuell möchte ich Sie darauf hinweisen, dass unter

http://www.datenschutzzentrum.de/vortraege/050301_weichert_telematik.pdf

eine **Power-Point-Präsentation** abrufbar ist, die ich am 02.03.2004 in Flensburg auf dem dortigen Telematik-Forum vorgestellt habe.

Im Folgenden nehme ich Stellung zu einigen Aspekten des in der o.g. E-Mail mitversandten Dokumentes.

Architekturentscheidungen - Auswertung der Vorprojekte und Empfehlungen für das FuE (Version 1.0 vom 07.02.2005:

Das Papier geht von der grundlegend falschen Annahme aus, die „**Datenhoheit** liegt beim Versicherten/Patienten“ (1.3 auf S. 4, 3.1 auf S. 12). Er sei „Sender und/oder Empfänger von jedem zur Realisierung einer eGK-Anwendung notwendigen Datentransport über die Telematikinfrastuktur“. Verantwortlich i.S.d. Datenschutzrechtes ist nur in wenigen Fällen (EPA) der Versicherte. In den meisten Fällen sind dies die Kassen (Stammdaten) bzw. Ärzte/Apotheker/Krankenhäuser usw. (Anwendungen). Auch im Rahmen der Datenverarbeitung im Auftrag dürfen die Verantwortlichkeiten i.S.d. Datenschutzrechtes nicht verunklart werden. Die Klärung der Verantwortlichkeiten ist grundlegend für sämtliche weiteren Architekturentscheidungen.

In dem Papier wird vorgeschlagen, dass die **Datenzuordnung zu einer Person** „nur über eine auf der eGK abgelegte Referenz“ erfolgen solle (1.3 auf S. 4). Neben der Kartennummer und der Versicherten-ID wird hier der „Pointer“ genannt. Da ein Pointer regelmäßig nicht auf eine Person, sondern auf ein Dokument verweisen dürfte, kann dies nicht richtig sein. Der Begriff „Versicherten-ID“ soll evtl. auf die Krankenversichertennummer nach § 290 SGB V verweisen. Wenn dies so ist, dann sollte die rechtlich korrekte Terminologie genutzt werden. Sollte nur der „unveränderbare Teil“ der KV-Nummer gemeint sein, so ist dies erkennbar zu machen.

Unter 2.1. (S. 6, 1. Spiegelstrich) wird postuliert, dass verschiedene Anwendungen, u.a. das eRezept, „das **Vorhandensein von eGK und HBA**“ erfordere. Dies kann nicht richtig sein, da beim eRezept eine Ausstellung (z.B. mit dem öffentlichen Schlüssel des Patienten durch den Arzt) auch in Abwesenheit des Patienten möglich sein soll.

Bzgl. der Prüfung von rollenspezifischen Zugriffsrechten wird auf das „**Triadenkonzept** über die eGK“ verwiesen (S. 6 6. Spiegelstrich). Dieses Konzept ist hier nicht bekannt.

Unter 2.6 wird in aus Datenschutzsicht falscher Terminologie zwischen „**personenbezogenen und medizinischen Daten**“ unterschieden. Solange medizinische Daten nicht anonymisiert sind, sind diese personenbezogen. Gemeint ist die Unterscheidung zwischen Identifikationsdaten (vgl. § 291 Abs. 2 SGB V) und sonstigen Daten (vgl. § 291a Abs.3 SGB V, insofern richtig auf S. 14). Ein zentraler Datenschutzaspekt ist nicht nur die physikalische Trennung zwischen Identifizierungs- und Medizindaten, wichtig sind auch deren Verknüpfung bzw. Verknüpfungsmöglichkeit über unterschiedliche Pseudonyme, der Umgang mit den Pseudonymen sowie technisch-organisatorische Sicherungen.

Unter 3.1 wird auf S. 14 postuliert, Datenschutz und **Datensicherheit** seien gemäß den „anerkannten Richtlinien und unter Einsatz moderner Technologien gewährleistet“. Gerade insofern hätte ich mir von einer Architekturentscheidung konkrete Aussagen erwünscht. Die unter 1. gemachten Ausführungen sind notwendig, aber bei Weitem nicht hinreichend. Allein die gesetzlich festgelegten Anforderungen gehen über die hier formulierten (getrennte Verwaltung, Verschlüsselung, Zugriffskonzept, Sicherung von Integrität und Authentizität) hinaus. In diesem Zusammenhang weise ich auf die Notwendigkeit der von mir thematisierten „Ende-zu-Ende-Verschlüsselung“ durch den Patienten hin. (siehe mein Schreiben vom 08.02.2005).

Mit freundlichen Grüßen

Dr. Thilo Weichert