

Betreff:

WG: "Meilensteine" des ATG; Stellungnahme des Bayerischen Landesbeauftragten für den Datenschutz; Az.: DSB 5 - 624 - 255

Datum: Mon, 7 Aug 2000 16:17:53 +0200

Von: Poststelle@Datenschutz-Bayern.de

An: j.dolle@gvg-koeln.de

Sehr geehrter Herr Dolle,

ich begrüße - auch im Namen des Bayerischen Landesbeauftragten für den Datenschutz Reinhard Vetter - , dass die bereits vorliegenden Managementpapiere (Meilensteine) des ATG in das Internet eingestellt und zur Diskussion freigegeben wurden. Dem Vorstand der IGD e. V. danke ich dafür, dass er in seiner Stellungnahme die Gesichtspunkte Vertraulichkeit und Datenschutz besonders benannt hat. Ich bin der Auffassung, dass die Akzeptanz der Telematik im Gesundheitswesen bei allen Beteiligten umso höher sein wird, je sicherer die technische Ausgestaltung der Anwendungen ist. Im einzelnen habe ich zu den Managementpapieren noch folgende Kommentare und Anregungen:

* Aus technischer Sicht teile ich die Anmerkungen von SBS zu dem "Managementpapier zum Elektronischen Arztbrief". Der Aufbau einer einheitlichen Sicherheitsinfrastruktur erscheint bei der Heterogenität der Betroffenen/Beteiligten als sehr ehrgeizig und auch in mittlerer Zukunft nicht umsetzbar. Zielführender erscheint mir der Ansatz, auf verfügbaren kommerziellen und sonstigen existenten Strukturen aufzubauen und für gegenseitige Interoperabilität dieser Systeme zu sorgen.

Die Aussage bei den rechtlichen Rahmenbedingungen (Nr. 3.1.), dass aufgrund der bestehenden Regelungen ein ausreichender Datenschutz gewährleistet ist, erscheint mir doch etwas verkürzt. In dem Papier sollten diese rechtlichen Rahmenbedingungen etwas umfassender als nur durch die Nennung einiger Vorschriften (Nr. 8.8) dargestellt werden. Ich rege daher noch folgende Ergänzungen - ohne Anspruch auf Vollständigkeit - an, die sinngemäß für alle telemedizinischen Anwendungen gelten:

Die Möglichkeit und der Wunsch Telemedizin zu betreiben, ändern nichts an den rechtlichen Grundlagen der Datenverarbeitung in der Medizin. Es kann also mit anderen Worten alleine der Wunsch nach der Umsetzung telemedizinischer Anwendungen die hiermit verbundenen Datenverarbeitungen nicht rechtfertigen. Auch in der Telemedizin gelten die selben rechtlichen Regelungen wie in der traditionellen - nicht vernetzten - Medizin. Zu beachten sind daher die in den Berufsordnungen für die Ärztinnen und Ärzte enthaltene ärztliche Schweigepflicht, die in § 203 Abs. 1 Nr. 1 StGB strafbewehrt ist. Relevant ist ferner der Grundsatz der Erforderlichkeit, der zunächst verlangt, zu beurteilen, ob überhaupt personenbezogene Daten verwendet werden müssen, oder anonymisierte oder pseudonymisierte (z. B. für Qualitätssicherungsverfahren) Daten ausreichen. Sollte die Übermittlung personenbezogener Daten erforderlich sein, stellt sich die

Frage, in welchem Umfang ärztliche Informationen übermittelt werden müssen. Für personenbezogene bzw. personenbeziehbare Datenverarbeitungen sind der Behandlungsvertrag, die (freiwillige und informierte) Einwilligung des Patienten, sowie die bereichsspezifischen (z. B. Krankenhausgesetze) und die allgemeinen Datenschutzgesetze zu beachten. Je nach Anwendungsbereich ist die ärztliche Kommunikation ggf. auch in den einzelnen Büchern des Sozialgesetzbuches (SGB) geregelt, vgl. etwa § 73 Abs. 1b SGB V (Hausarztmodell) und § 140a Abs. 2 SGB V (Integrierte Versorgung).

* Bezüglich des "Managementpapiers zur Sicherheitsinfrastruktur" habe ich folgende Bemerkungen:

Aus technischer Sicht teile ich die Anmerkungen von SBS. Auf obige Ausführungen weise ich hin.

Zur als notwendig betrachteten Konformität mit dem derzeitigen Signaturgesetz (Nr. 3.2.1) verweise ich auf die derzeitige Novellierung des SigG und den Gesetzentwurf zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr und auf die daraus resultierenden momentanen Unwägbarkeiten.

Die oben dargestellten rechtlichen Vorgaben gelten natürlich auch hier. Ergänzend weise ich auf die Anforderungen des BDSG und der Landesdatenschutzgesetze an technische und organisatorische Maßnahmen der Datensicherheit hin (z. B. "10 Gebote" des § 9 BDSG i. V. m. der Anlage hierzu).

* Zur Studie "Europäische und Internationale Dimension von Telematik im Gesundheitswesen" möchte ich die Empfehlungen auf Seite 22 dahingehend kommentieren, dass in der Tat diejenigen Informationssysteme Unterstützung erhalten sollten, die einen (auch Datenschutz-)mündigen und im Hinblick auf seine vitalen Interessen bedachten Patienten favorisieren. Ich erachte es zur Gewährleistung des Vertrauensverhältnisses zwischen Arzt und Patient und zum Schutz der Patientendaten für zwingend erforderlich, dass jeder Patient weitestgehende Kontrollmöglichkeiten über ihn betreffende Datenspeicherungen hat (insbesondere durch Erfüllung seiner Auskunftsrechte) und selbstverantwortlich entscheiden kann, welche Daten wo von wem zu welchem Zweck verwendet werden dürfen.

Erhebliche rechtliche Bedenken habe ich bezüglich der Einführung einer lebenszeitlichen, einheitlichen Personenkenzziffer (Seiten 22 und 14 der Studie) in Deutschland. Wie das Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 festgestellt hat, wäre die Erschließung eines Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal problematisch, da eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger - sogar in der Anonymität statistischer Erhebungen - unzulässig ist (NJW 1998, S. 424). Selbst "Teilabbilder" der Persönlichkeit anzufertigen, ist nach dieser Entscheidung problematisch (BVerfG a.a.O.).

Aus Gründen der Datensicherheit sind einer zentralen Patientendatenhaltung verteilte elektronische Patientenakten, deren einzelne Komponenten sich bei den jeweiligen Leistungserbringern befinden und die bei Bedarf zusammengefügt werden können (sogenannte "Virtuelle Patientenakten"), datenschutzrechtlich vorzuziehen.

Mit freundlichen Grüßen

I.A.

gez.
Dr. Pfister

Geschäftsstelle des Bayer. Landesbeauftragten für den Datenschutz
Wagmüllerstraße 18 - 80538 München
Postfach 22 12 19 - 80502 München
Tel. +49 89 212672-0 Fax +49 89 212672 50