ELGA statt Datenschutz?

Hans G. Zeger, ARGE DATEN

Gmunden, Medizinrechtskonferenz 11./12. Mai 2012

Es sind nicht die Daten vor den Menschen zu schützen, sondern den Menschen ist in der Informationsgesell-schaft das Grundrecht auf Privatsphäre zu sichern.

Art. 1 Abs. 1 "Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten."

("Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (Datenschutzrichtlinie 95/46/EG)

Dr. Hans G. Zeger

© ARGE DATEN 2012

eHealth international

ELGA ist nicht EU-eHealth !

eHealth-Entwicklungen:

- Gesundheitsportale für/von Laien, Selbsthilfegruppen, Gesundheitsdiensteanbieter
- Onlinedienste: Onlineordinationen, Videodiagnostik, Online-Apotheke, Online-Archive, ...
- Telemedizin, IT-gestützte Heimbetreuung: Real-Time-Überwachung von Vitalfunktionen
- Remote Assisted Healthcare: Expertenunterstützung, ...
- iMedikation, ubiquitäre Gesundheitsversorgung: individuell hergestellte Medizinprodukte inkl. Compliance-Programme

Man kann zu diesen Themen stehen wie man will. Fakt ist, sie werden nachgefragt, sie werden angeboten und sie werden gefördert!

Dr. Hans G. Zeger

Entwurf ELGA-Gesetz

Einige ungelöste ELGA Fragen

- **Verantwortung**: wird pauschal dem GDA zugewiesen, gleichzeitig werden ihm die Handlungsspielräume nach DSG 2000 entzogen, umgekehrt sind zentrale ELGA-"Spieler" (die ELGA-Systempartner) völlig von der Verantwortung ausgenommen
- **Zweck**: es existiert keine saubere Trennung zwischen verschiedenen Zwecken (Dokumentation, Behandlung, Abrechnung, Haftung, Qualitätssicherung, Controlling, ...)
- **Sicherheit**: Wiederholung der vagen § 14 DSG 2000 Bestimmungen oder doch Präzisierung? Es gibt kein Zertifizierungskonzept für Verwaltung und Übermittlung der Daten, "Selbstzertifizierung" birgt Gefahr der Nivellierung nach unten, widerspricht internationalen Entwicklungen

Dr. Hans G. Zeger

Einige ungelöste ELGA Fragen II

- **Projektabwicklung**: nicht Stand der Technik, keine geordnete Enwicklung von Zweckdefinition ⇨ Schaffung gesetzlicher Rahmen ⇨ Pflichtenheft ⇨ Ausschreibung ⇨ Auftragsvergabe inkl. Trennung von Planung, Entwicklung, Betrieb und Aufsicht
  undurchsichtige Vermengung dieser Aufgaben durch ein (sozialpartnerschaftliches?) ELGA-Systempartner-Gremium
- **Gefahr der Abhängigkeit** der GDAs von Software-Lieferanten: kann nur durch konsequente Vorgabe und Durchsetzung von Schnittstellen, Standards gelöst werden

Einige ungelöste ELGA Fragen III

- **Informed Consent der Patienten**: völlig ungeklärt ist, wer die Aufklärung der Patienten zur ELGA-Teilnahme übernimmt, bedeutet enormen Aufwand wenn tatsächlich alle medizinischen und informationstechnischen Fragen und Konsequenzen geklärt werden
- **eHealth**: internationale Entwicklungen zu eHealth werden ignoriert, ELGA ist als statisches Listensystem konzipiert
- **Identifikation**: Existenzberechtigung eines eigenen Patientenindex fraglich, sollte zur Neuorganisation der Patientenidentifikation Anlass geben
- **...**

ELGA-NEU

Eine optimale ELGA-Lösung - Voraussetzungen

- ELGA sollte jedenfalls seinem Namen gerecht werden ⇨ System muss vollständige Dossiers verwalten, die nach den Bedürfnissen des individuellen Patienten maßgeschneidert sind
- Patientendossier ist kein Behandlungsakt ⇨ hat eigenständigen Zweck (Patientendokumentation), damit werden Abgrenzungs- und Berechtigungsprobleme vermieden
- ELGA ist keine "eierlegende Wollmilchsau" ⇨ Zwecke wie Qualitätssicherung, Abrechnung, Behandlung, Leistungskontrolle und Haftung verlangen völlig unterschiedliche Datenstrukturen, Behaltezeiträume, Änderungs- und Zugriffsrechte
- Reduktion der Komplexität sollte Ziel von ELGA-NEU sein

Weil das BMG die Reformfähigkeit in der Gesundheits-versorgung negativ einschätzt, wird versucht durch einen großen Befreiungsschlag alle Probleme abzudecken

Dr. Hans G. Zeger

ELGA-NEU

Eine optimale ELGA-Lösung - Eckpfeiler

- mehrere zertifizierte Anbieter von ELGA-Portalen für die Verwaltung der Dossiers
- Freiwilligkeit der Patienten und GDAs mit klar definierten Informations- und Zustimmungspflichten
- alle Dossiers eines Patienten in einem System (Reduktion der Komplexität!)
- Dossiers werden revisionssicher und beschlagnahmesicher abgelegt (Signatur und Verschlüsselung)
- einfaches und umfassendes Berechtigungs-, Löschungs-, Ergänzungs- und Richtigstellungssystem für den Patienten
- strikte Trennung zwischen Dokumentation für Betreuungs-/Behandlung und sonstigen Aufgaben (Kostenrechnung, Controlling, Qualitätssicherung, Forschung, Weiterentwicklung des Gesundheitssystems)

Dr. Hans G. Zeger

ELGA-NEU

Eine optimale ELGA-Lösung - Rollenverteilung I

ELGA-Portal:

- zertifizierter Betreiber ist Auftraggeber im Sinne des DSG für Verwaltung des Archivs, des Nachweises der Herkunft der Daten, der Zugriffe, der Berechtigungen usw, nicht für Inhalte,
- Arzt/GDA übermittelt im Sinne des DSG, Dokumentation der Herkunft der Daten bleibt erhalten (Signatur/Authentizität),
- Patient authorisiert Empfänger, Patient ordnet, erweitert und sperrt Dokumente, Zweck ist Erstinformation authorisierter Empfänger im Behandlungsfall (inkl. Rechtevergabe für Notfälle, Patientenverfügungen usw.)
- Patient definiert Vertreter (z.B. Angehörige, Vertrauensärzte, ...) die in besonderen Situationen (Notfall, nicht ansprechbar, ...) seine Rolle übernehmen

Patient ist, soweit es seine eigenen Daten betrifft weder Betroffener, Auftraggeber noch Dienstleister!

Dr. Hans G. Zeger

ELGA-NEU

Eine optimale ELGA-Lösung - Rollenverteilung II

ELGA-Dienstleister (nach Ausschreibung ELGA-GmbH?):

- definiert Zertifizierungsrichtlinien und -abläufe
- definiert Schnittstellen
- beobachtet internationale Entwicklung im Zusammenhang mit eHealth
- übernimmt Informations- und Koordinationsaufgaben zwischen den ELGA-Portalen
- betreibt eine Plattform mit anonymisierten Daten aus den ELGA-Portalen für Zwecke der Qualitätssicherung, Controlling, ..
- betreibt Zugangsportal für qualitätsgesicherte Gesundheitsinformationen [vergleiche § 23 GTelG Entwurf]

Dr. Hans G. Zeger

Eine optimale ELGA-Lösung - Rollenverteilung III

Auditoren / Zertifizierungsstellen:

- prüfen Betreiber der Portale und führen Zertifizierungen durch

strenge Trennung zwischen Definitionsstelle von Zertifizierungsvorgaben, Zertifizierungsstellen und Portal-Betreibern muss selbstverständlich sein

BMG:

- schafft die erforderlichen rechtlichen Grundlagen zum Einsatz von Standards, Sicherheitsmaßnahmen, ... (Gesetze, Verordnungen)

... die schlechte Nachricht zuletzt ...

... für die ELGA-Systempartner ist mir bei bestem Willen keine - im Sinne des DSG 2000 - verantwortliche Rolle eingefallen

Sicherheitsbestimmungen (§ 14)

Sicherheitsmaßnahmen haben einen Ausgleich zwischen folgenden Punkten zu finden:

Stand der Technik entsprechend
wirtschaftlich vertretbar
angemessenes Schutzniveau muss erreicht werden

rechtlich-organisatorische Sicherheitsmaßnahmen

- ausdrückliche Aufgabenverteilung
- ausschließlich auftragsgemäße Datenverwendung
- Belehrungspflicht der Mitarbeiter
- Regelung der Zugriffs- und Zutrittsberechtigungen
- Vorkehrungen gegen unberechtigte Inbetriebnahme von Geräten
- **Protokollierungspflicht soweit für die rechtmäßige Datenverwendung erforderlich**

ELGA - Sicherheitsanforderungen

- müssen detaillierter sein als im DSG 2000 vorgesehen
- müssen auf spezifische Probleme von Gesundheitsdaten eingehen (flächendeckende Verfügbarkeit, besondere Integritätsanforderungen, ...)
- müssen alle Datenverwendungen abdecken (inkl. Übertragung, Speicherung, Berechtigungsverwaltung)
- ein Auftraggeber muss für alle Aspekte verantwortlich sein!
- ELGA-Entwurf enthält keine objektivierbaren Sicherheitsvorgaben
- vorgesehene "Selbstverwaltung" der IT-Sicherheit durch Rechtsträger, Aufsichts- oder Kontrollbehörden [§ 8 Abs. 2 GTelG Entwurf] birgt Gefahr der Nivellierung nach unten

ELGA - Sicherheitsanforderungen II

- IT-Sicherheitslösungen in kritischen Anwendungen erfolgt üblicherweise durch sogenannte Schutzprofile, etwa gemäß Common Criteria
  ⇨ internationale Entwicklung wird ignoriert
- Plattformen mit erhöhtem Schutzbedarf (z.B. bei sensiblen Daten) erfordern Zertifizierungen, etwa nach ISO 27001
  ⇨ verlangen zwingend einen Verantwortlichen!

im Gegenteil: ELGA Leitlinie 001 zur Sicherheitspolitik stellt fest, gegenwärtige Konstruktion erlaubt keine Zertifizierung!

- übliche Standards verlangen völlige Trennung zwischen Stellen, die Sicherheitsvorgaben (Leitlinien, Policies, ..) erstellen und diese anwenden
  ⇨ bei ELGA gibt sich ELGA GmbH selbst die Sicherheitsvorgaben, es gibt keine unabhängige und weisungsbefugte Kontrollstelle

Ich danke für Ihre Aufmerksamkeit

Kontaktinformationen

Dr. Hans G. Zeger
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
A-1160 Wien, Redtenbachergasse 20

Tel.: 01 53 20 944
Fax.: 01 53 20 974
Mail persönlich: hans.zeger@argedaten.at

Website: http://www.argedaten.at
Zertifizierung: http://www.a-cert.at
e-commerce: http://www.e-rating.at

DSG2000: http://www.argedaten.at/dsg2000
diverse Muster: http://www.argedaten.at/muster/