BUNDESMINISTERIUM
FÜR GESUNDHEIT

Regierungsvorlage ELGA: Garantien für Datenschutz und Datensicherheit

Selbstbestimmungsrecht

- Möglichkeit des kompletten Ausstiegs (Widerspruchsrecht §15 Abs. 2)
- Verhinderung der Speicherung in ELGA im Einzelfall (§ 16 Abs. 2 Z 2)
- Möglichkeit Daten in ELGA unsichtbar zu machen oder nachträglich zu löschen (§ 16 Abs. 1 Z 2 lit.a)
- Diskriminierungsverbot bei Widerspruch (§16 Abs. 3)
- Nur für Behandlung und Betreuung wesentliche Daten und absoluter Ausschluss von psychischen Geheimnissen (§10 Abs. 4 KAKuG) und Genanalysen (§71a Abs. 2 GTG) (ELGA-Gesundheitsdaten §2 Z 9)
- Widerspruchsstellen und PatientInnenportal müssen vor Betrieb von ELGA eingerichtet werden (§27 Abs. 1)
- ELGA-Ombudsstelle unterstützt Menschen ohne Internetzugang und bei Datenschutzproblemen (§17)

Transparenz

- Informationspflicht über Widerspruchsrechte durch LIVE-Information (§81 ASVG), Minister (§16 Abs. 5), Aushang in Räumlichkeiten wie z.B. Ordinationen (§16 Abs. 4) sowie bei besonders sensiblen Daten wie HIV oder psychischen Erkrankungen durch Gesundheitspersonal (§ 16 Abs. 2 Z 2)
- Lückenlose Protokollierung welche natürliche Personen auf ELGA zugegriffen haben (§22 Abs. 2 Z 5)
- Einsichtsrecht der PatientInnen in die Protokolle (§22 Abs. 4)
- Zugriff der PatientInnen auf eigene Daten (§14 Abs. 2 Z 2 lit. a)

Eindeutige Identifizierung und Zugangsberechtigungen

- PatientInnen müssen immer technisch unter deren Mitwirkung zweifelsfrei identifiziert werden (§18 Abs. 4)
- BenutzerInnen müssen zweifelsfrei identifiziert werden (§19 Abs. 2)
- Zugriff nur bei Nachweis eines Behandlungszusammenhanges (§14 Abs. 1)
- Modulare Zugangsrechte, z.B. Apotheken nur Medikamentenliste (§21 Abs. 2)
- PatientInnen können Berechtigungen individuell festlegen (§21 Abs. 3)

18. Oktober 2012

Verwendungsverbote und Strafen

- Verwendung nur zur Behandlung und Betreuung erlaubt (§14 Abs. 2)
- Verwendungsverbot für Versicherungen, Arbeitsmediziner etc. (§14 Abs. 3)
- Vorgaben für Gesundheitseinrichtungen gegenüber eigenen MitarbeiterInnen (§14 Abs. 3a)
- Spezielle ELGA Verschwiegenheitspflicht (§14 Abs. 4)
- durch Strafbestimmungen abgesichertes Verbot jedes Zugriffs für Zwecke, die nicht ausdrücklich durch Gesetz erlaubt sind (§25)
- durch Strafbestimmungen abgesichertes Verbot Gesundheitsdaten zu verlangen, z.B. Arbeitgeber (§121 StGB)

Datensicherheit

- Datentransport nur verschlüsselt oder abgesicherte Netze (§6 Abs. 1)
- Datenspeicherung beim „Cloud Computing" nur verschlüsselt (§6 Abs. 3)
- Verbindliches IT-Sicherheitskonzept für alle Gesundheitseinrichtungen, sodass Unbefugten Gesundheitsdaten nicht zugänglich sind (§8 Abs. 1)
- Technische und organisatorische Vorschriften über die Sicherheitsanforderungen und Zugriffsschutz nur am neuesten Stand per Verordnung (§28 Abs.2 Z 5), wie z.B.
    - manipulationssichere Speicherung,
    - sichere kryptografische Verschlüsselungsverfahren,
    - systematische Kontrolle der Protokolle auf missbräuchliche Zugriffe
- Datenspeicher nur in der EU (§20 Abs. 1)
- dezentrale Speicherung der Befunde (§20 Abs. 3)
- Administrator- und EDV-Wartungszugriffe nur auf verschlüsselte Daten oder 4-Augen-Prinzip (§28 Abs.2 Z 5)
- ELGA-Systempartner (Bund, Länder SV) haben ein verbindliches Informationssicherheits-Management System (ISMS) für alle Betreiber von ELGA-Komponenten entwickelt
    - ELGA-Sicherheitskommission bündelt Sicherheitsexpertise
    - Verfügbarkeit eines Computer Emergency Response Teams (CERT) mit 24h Einsatzfähigkeit
    - Leitlinien für Sicherheitspolitik- und organisation
    - Sicherheitsaudits