Orientierungshilfe Krankenhausinformationssysteme

Informationsaustausch mit Vertretern der Krankenhäuser in Thüringen

am 22.05.2012
im Thüringer Landtag

Referentin:

Sabine Pöllmann

Referatsleiterin beim

Thüringer Landesbeauftragten für den Datenschutz

Tel.: 0361-3771921

Fax: 0 361 / 37 71 904

: poststelle@datenschutz.thueringen.de

Gliederung

1. Rechtliche Grundlagen
2. Entstehung der Orientierungshilfe
3. Entwicklung in Thüringen
4. Normative Eckpunkte im Einzelnen unter Berücksichtigung der in den kontrollierten Krankenhäusern gemachten Erfahrungen
5. Ausblick

Rechtliche Grundlagen:

- Subsidiarität des Thüringer Datenschutzgesetzes, § 2 Abs. 3 ThürDSG
- Thüringer Krankenhausgesetz (§§ 27 -27b)
- ergänzend: ThürDSG oder BDSG
- § 203 StGB

ThürDSG oder BDSG?

- Krankenhäuser in rein privater Trägerschaft – Anwendbarkeit des BDSG

- Krankenhäuser in (teilweise) öffentlicher Trägerschaft

  - Nach § 2 ThürDSG eigentlich ThürDSG anwendbar

  - wegen § 26 ThürDSG

    - Fünfter Abschnitt ThürDSG (ohne § 34 Abs. 2)

    - ansonsten BDSG mit Ausnahme des Zweiten Abschnitts und des § 38.

Konsequenzen

- Bei direkter Anwendbarkeit des BDSG

  - Maßnahmen nach § 38 BDSG
    - Anordnung von Maßnahmen
    - Androhung von Zwangsgeld
    - Abberufung des Beauftragen für den Datenschutz

  - Ordnungswidrigkeitenverfahren nach § 43 BDSG (Bußgeld bis zu 300.000 €)

  - Strafantrag, § 44 Abs. 2 Satz 2 BDSG

Konsequenzen

- Bei Anwendbarkeit über § 26 ThürDSG

  - Maßnahmen nach §§ 37 ff. ThürDSG
    - Beanstandung
    - Einbeziehung der Aufsichtsbehörde
    - Information des Landtags und der Landesregierung

  - Ordnungswidrigkeitenverfahren nach § 43 BDSG (Bußgeld bis zu 300.000 €)

  - Strafantrag, § 44 Abs. 2 Satz 2 BDSG

Entstehung der Orientierungshilfe

- Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK)
- Bildung einer Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“
- Erarbeitung der Orientierungshilfe unter Berücksichtigung der Vorstellungen der Krankenhäuser und der Hersteller
- Verabschiedung auf der 81. DSK am 15./16. März 2011
- Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 04./05. Mai 2011)

Entwicklung in Thüringen

- Abfrage bei den Krankenhäusern in öffentlicher Trägerschaft
  - Größe und Struktur des Krankenhauses
  - Verwendetes KIS
  - Subsysteme
  - Auftragsdatenverarbeitung
- Auswahl der zu kontrollierenden Krankenhäuser

Entwicklung in Thüringen

- Erarbeitung eines Fragenkatalogs anhand der OH KIS
- Besuch in sechs Krankenhäusern (jeweils 2 Tage)
- Erstellen der Kontrollberichte
- Dialog zur Umsetzung

Aufbau der Orientierungshilfe

- Begleitpapier
- Glossar
- Teil I: Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus
- Teil II: Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

OH KIS – Normative Eckpunkte

Aufnahme

- Administrative Aufnahme

  - Suchfunktion – nur Identifikationsdaten
  - Zugriff auf vorbehandelnde Organisationseinheit nur wenn Behandlungsfall noch nicht abgeschlossen
  - Warnhinweis – möglichst standardisiert
  - Widerspruchrecht in Bezug auf die Hinzuziehung von Vorbehandlungsdaten
  - Basisdatensatz
  - Auskunftssperre

Aufnahme

- medizinische Aufnahme – Erhebung von medizinischen Daten
  - Hinweis im System, ob Heranziehung der Vorbehandlungsdaten widersprochen wurde
  - Mutmaßliche Einwilligung im Notfall bzw., wenn der Patient nicht ansprechbar ist.

Behandlung

- Jede an der Behandlung oder Verwaltung des Patienten beteiligte Person darf auf Identifikationsdaten zugreifen.

- Bei medizinischen und Pflege-Daten ist nach dem Rollen- und Berechtigungskonzept zu differenzieren.

Zugriff durch Ärzte

- Fachliche oder räumliche Zuordnung eines Patienten zu einem Arzt oder einer Gruppe von Ärzten (Organisationseinheit)

- Erweiterung des Kreises der Zugriffsberechtigten auf Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes ab dem Zeitpunkt des konkreten Behandlungsauftrags.

- Bei Wechsel zu einer anderen Organisationseinheit i. d. R. nur Zugriff auf die „alten“ Daten

Zugriff durch Ärzte

- Für nur zeitweise erweiterte Zugriffserfordernisse sollten Berechtigungen befristet und nur für den jeweiligen Zuständigkeitsbereich zugewiesen werden.

- Berechtigung, auch nach Ende des Patientenkontakts auf die Dokumentation der eigenen Leistungen zuzugreifen.

- Konsilanforderungen dürfen den Datenzugriff nur in Bezug auf den betroffenen Patienten eröffnen, für

  - einen einzelnen Arzt
  - eine vorab definierte Gruppe von Konsiliardienstleistenden

Zugriff durch Ärzte

- Ein Notzugriff auf Patientendaten ist außerhalb eines differenzierten Berechtigungskonzepts nicht erforderlich.

- Notfallzugriff nur, wenn

  - automatisch ein Hinweis darüber aufklärt, dass ein Zugriff außerhalb der Berechtigung erfolgt,
  - einen Zugriffsgrund anzugeben ist und
  - der Zugriff protokolliert und
  - anschließend kontrolliert wird.

- Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten.

Zugriff durch Pflegepersonal

- Zugriff des Pflegepersonals ist zu begrenzen auf
  - die erforderlichen pflegerischen und medizinischen Daten
  - der in der eigenen funktionsbezogenen Organisationseinheit behandelten Patienten
- Springer; Zuweisung muss dokumentiert werden
- Verlegung ist mit tatsächlichem Zugriffswechsel verbunden.

Fachübergreifende Zugriffe

- Mitarbeiter mit fachrichtungsübergreifender Funktion sollten Daten-Zugriff entweder durch individuelle Zuweisung oder durch den Patientenkontakt erhalten.

- Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren.

- Das (Zentral-)Labor darf mit der Leistungsanforderung nur einen Zugriff auf die für die Befundung erforderlichen erhalten.

Nach der Behandlung

- Nach Abschluss des Behandlungsfalles ist die elektronische Patientenakte zu sperren.
- Es ist notwendig, für die Sperrung eine feste Frist nach Entlassung des Patienten festzulegen.
- Von der Sperrung ausgenommen sind lediglich die Identifikationsdaten.

Nach der Behandlung

- Auf gesperrte Daten darf nur ein eingeschränkter Personenkreis Zugriff erhalten, um festgelegte Aufgaben erfüllen zu können
- Die Zugriffsberechtigungen für diese Zwecke zeitlich begrenzen
- Patientensuche in gesperrten Daten ist nur nach wenigen vorgegebenen Kennzeichen (z.B. Name, Entlassungsdatum) zu ermöglichen

Nach der Behandlung

- Eine Übertragung dieser Aufgaben und Zugriffsrechte auf ein zentrales Patientenmanagement bedarf zusätzlicher Sicherungsmaßnahmen

- Patientendaten sind zu löschen, wenn

  - sie zur Durchführung des Behandlungsvertrags nicht mehr erforderlich sind,
  - vorgeschriebene Aufbewahrungsfristen abgelaufen sind und
  - kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Zugriffe durch Funktionskräfte

- Zugriff nur auf die jeweils erforderlichen Patientendaten
- Soweit Zugriff auf alle Daten eines Patienten zugelassen werden muss, ist durch Zuständigkeits- und Funktionsaufteilungen und zeitliche Beschränkungen ein ständiger Vollzugriff zu vermeiden.
- Soweit möglich Verwendung, bei der die Identitätsdaten des Patienten nicht zur Kenntnis genommen werden können.

Sonstige Zugriffe

- Aus- und Fortbildung; i. d. R. Anonymisierung der Daten oder Einwilligung, § 27 Abs. 1 ThürKHG
- Andere Krankenhäuser oder Unternehmen des Konzerns (MVZ) – verschiedene Mandanten
- Sonderproblem Schreibkraft

Technische Administration

- Zugriffsrechte und Eingriffsebenen der Administratoren sind nach Aufgaben zu begrenzen
- Aktivitäten sind revisionsfest zu protokollieren
- Für die Nutzung von Protokolldaten ist ein Auswertungskonzept zu erstellen
- Remote-Zugriff nur mit Kenntnis und Einwilligung der Betroffenen
- Fernwartung nur mit Wissen und Wollen des Krankenhauses

Besonders schutzwürdige Patientengruppen

- Krankenhaus-Mitarbeiter; Zugriff nur der unmittelbar an der Behandlung Beteiligten
- VIPs; Festlegungen der Klinikleitung erforderlich.
- Ambulant in Nebentätigkeit behandelte Privatpatienten; soweit die Daten dieser Patienten im KIS verarbeitet werden, sind sie getrennt von den übrigen Daten zu halten.

Zugriffsprotokollierung und Datenschutzkontrolle

- aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe sowie geeignete Auswertungsmöglichkeiten
  - Zugriffe aus der fachlichen Verfahrensnutzung
  - Zugriffe der administrativen Betreuung
- Grundsatz der Erforderlichkeit; Art, Umfang und Dauer der Protokollierung sind auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken
- stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle

Auskunftsrechte des Patienten

§ 27 Abs. 8 ThürKHG:

- Den Patienten ist auf Antrag kostenfrei Auskunft über die zu ihrer Person gespeicherten Daten sowie über die Personen und Stellen zu erteilen, an die personenbezogene Daten weitergegeben wurden.

- Auskunft darüber, welche Patientendaten zur Behandlung oder zu deren verwaltungsmäßiger Abwicklung übermittelt wurden, ist zu erteilen, soweit die Unterlagen des Krankenhauses hierzu Angaben enthalten.

- Die Auskunft soll im Einzelfall durch die Ärzte vermittelt werden, soweit dies mit Rücksicht auf den Gesundheitszustand der Patienten dringend geboten ist.

- Eine Beschränkung der Auskunft nach Satz 1 hinsichtlich ärztlicher Beurteilungen oder Wertungen ist zulässig.

Ausblick

- Weitere Begleitung der kontrollierten Krankenhäuser
- Fortentwicklung der OH KIS
- Kontrolle auch der Häuser in privater Trägerschaft
- Regelmäßige Arbeitsgruppensitzungen in Thüringen?