Cybersicherheit, Datenschutz und Ethik in der medizinischen Praxis

- Interessenkonflikte am Beispiel Krankenhaus

Workshop on Ethics and Cybersecurity in Health Care
am 24. April 2018 in Regensburg

David Koeppe - Datenschutzbeauftragter

Ihr Referent

David Koeppe
Konzerndatenschutzbeauftragter (GDDcert)
Vivantes - Netzwerk für Gesundheit GmbH
Aroser Allee 72-76
13407 Berlin
Tel.: 030/130-111011
Fax: 030/13029-111011
Mail: david.koeppe@vivantes.de

Leiter des Arbeitskreises „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Leiter des Erfa(hrungsaustausch)-Kreises Berlin der GDD

Agenda

Agenda

1. Rechtliche Ausgangssituation

2. Organisatorischer Rahmen

3. Interessenkonflikte + Handlungsfelder

4. Fazit

Rechtliche Ausgangssituation

Gesetzliche Verpflichtungen

Zu Datenschutz und Datensicherheit: EU-Datenschutz-Grundverordnung, insb.:

- Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 5 Grundsätze der Verarbeitung
- Art. 32 Sicherheit der Verarbeitung

Krankenhausgesetze der Länder

Speziell zur Informationssicherheit: IT-Sicherheitsgesetz (sofern KRITIS)

- § 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- § 10 Verordnungsermächtigung: BSI-Kritis-VO

Allgemein: Compliance-Vorschriften

- handels- und gesellschaftsrechtliche Compliance-Pflichten
- Governance-Auflagen von Ländern und Kommunen

Vivantes

Organisatorischer Rahmen

Ethik im Krankenhaus

„Ethik“ ist erst einmal eine Dimension in der Medizin

- In der Forschung - *institutionalisiert*
- Bei grenzwertigen medizinischen Entscheidungen
- In der Technisierung/Entmenschlichung der Medizin
- In der gesellschaftlichen Diskussion z.B. um Rationierung in der Medizin

Ethik im Zusammenhang mit der betrieblichen Informationssicherheit (z.B. durch „Value Sensitive Design“) hat in der betrieblichen Praxis bislang keine ausdrückliche Relevanz.

Organisatorischer Rahmen

Wo findet „Ethik“ im genannten Kontext statt?

- Anträge an die Ethikkomission (Forschung, klinische Studien)
  - teilweise, eher beiläufige Beachtung des Datenschutzes
  - Informationssicherheit ist häufig kein Thema
- Mitbestimmung (*Beschäftigten*datenverarbeitung)
  - Partielle und diffuse Einforderung des Datenschutzes
  - Informationssicherheit bisher selten ein relevantes Thema
  - Patientendatenverarbeitung ist außen vor
- Beschwerden über Arbeitsbehinderung anlässlich von Maßnahmen zur Informationssicherheit
  - Auto-Logoff, Passwort-Policies
  - Berechtigungsbeschränkungen

Interessenkonflikte Klinische Forschung

Fokus Forschung:

- (tendenziell) Datenmaximierung - Aufdeckung von Korrelationen
- Kostenminimierung - administrative Aufwandsminimierung

Fokus Datenschutz:

- Rechtmäßigkeit der Verarbeitung - meist Einwilligungserfordernis, Problem der „Pseudo-Anonymisierung“
- Grundsatz der Datenminimierung - Rechtfertigungszwang und Datenverzicht
- Grundsatz der Transparenz: Information, Gewährung Betroffenenrechte - administrativer Aufwand

Fokus Sicherheit:

- Pseudonymisierung als eine Sicherheitsmaßnahme - partieller Datenverzicht
- Technische Sicherheit trotz pseudo-anonymen Daten erforderlich

Handlungsfelder Klinische Forschung

Betrieblich

- Schaffung von Regelungen und Prozessen zur Sicherstellung der Rechtskonformität
- Sensibilisierung und Schulung der Forschenden - Bewertung des Konflikts
- Unterstützung der Forschenden bei administrativen/rechtlichen/technischen Ausgestaltungserfordernissen

Überbetrieblich

- Verstärkte Berücksichtigung des Datenschutzes in Ethikvoten
- Datenschutz und -sicherheit als Themen für Ärztekammern, Fachgesellschaften
- Forschung und Methodenentwicklung zu Pseudonymisierung, Umgang mit Big Data…
- Gesetzgeberische Bemühungen zum Rechtsrahmen für die Forschung

Interessenkonflikte bei Zugriffsberechtigungen auf Behandlungsdaten

Fokus Behandlung

- „Alle“ Daten müssen abrufbereit sein - Patientenwohl/-sicherheit, Haftung des Behandlers
- Zunehmend Zugriffe von außerhalb des Krankenhauses - ständige/bequeme Erreichbarkeit, Remote Access

Fokus Datenschutz

- Grundsatz der Vertraulichkeit - Einschränkung auf das „Behandlungsteam“
- Grundsatz der Datenminimierung - Eröffnung lediglich partieller Sichten
- Selbstbestimmungsrecht des Patienten - Verweigerung der Zustimmung des Zugriffs auf Vorbehandlungsdaten

Fokus Sicherheit

- Minimierung der Anzahl der Zugriffskanäle - keine Öffnung gegenüber dem Internet

Handlungsfelder bei Zugriffsberechtigungen auf Behandlungsdaten

Seitens der Einrichtung

- Schaffung von Awareness - Schulungen in Datenschutz und Informationssicherheit
- Anpassen der (klinischen) Prozesse an das Erfordernis restriktiver Berechtigungsprofile - „Aushalten“ von betrieblichen Konflikten

Seitens der Industrie

- Schaffung „intelligenter“ Mechanismen zur Berechtigungssteuerung: ort-, zeit- und situations-/prozessabhängig

Interessenkonflikte bei der Protokollierung von Datenzugriffen

Fokus Einrichtung

- Möglichst umfassende Protokollierung - Verantwortungszuweisung, Vermeidung eines Organisationsverschuldens

Fokus Datenschutz

- Grundsatz der Transparenz der Datenverarbeitung - Nachvollziehbarkeit aller Zugriffe und Verarbeitungstätigkeiten
- Entstehen einer weiteren Gruppe von betroffenen Personen
- Vermeidung von Vorrichtungen, die eine Leistungs- oder Verhaltenskontrolle ermöglichen - Dateminimierung, Mitbestimmungserfordernis

Fokus Sicherheit

- umfassende Protokollierung - Möglichkeit zur Aufdeckung von Problemen sowie Abschreckung

Handlungsfelder bei der Protokollierung von Datenzugriffen

Betrieblich

- Bewusste Ausgestaltung von Protokollierungen statt Hinnahme von teilweise unzureichenden oder nutzlosen Voreinstellungen des Herstellers
- Einforderung von Privacy by Design/Default bei der Produktbeschaffung

Speziell: Beschäftigtenvertretung

- Sensibilität im Umgang mit Protokollierungsfunktionen - stärkere Berücksichtigung bei der Ausübung der Mitbestimmung

System-Hersteller

- Privacy by Design/Default - Berücksichtigung von Datenschutzprinzipien bei der Produktentwicklung (gerne im vorauseilenden Gehorsam)

Fazit

Würdigung ethischer Aspekte im Krankenhaus im Spannungsfeld zwischen Informationssicherheit, Datenschutz und den Interessen der Einrichtung bzw. der Beschäftigten

- Das Anwenden von Paragraphen führt alleine meist zu keinem wertehaltigen Interessenausgleich.
- Das Nicht-Anwenden auch nicht.

Es bedarf:

- der Schaffung von Awareness auf allen Ebenen,
- des Raums für Diskurse zu Werten, nicht nur zu Ergebnissen,
- der Stärkung des klassischen Instrumentariums für betrieblichen Interessenausgleich: Mitbestimmung.

Ziel:

- „Bessere“, werthaltige Entscheidungen

Vielen Dank für Ihre Aufmerksamkeit