TELEMEDIZIN

EU-RECHT, BUNDES - UND LANDESRECHT: WAS GILT FÜR WEN UNTER WELCHEN UMSTÄNDEN

Dr. Bernd Schütze

GMDS Jahrestagung: München, 30. August 2016

HEALTHCARE SOLUTIONS

DR. BERND SCHÜTZE

Studium

- Studium Informatik (FH-Dortmund)
- Studium Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Studium Jura (Fern-Uni Hagen)

Zusatz-Ausbildung

- Zusatzausbildung Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Zusatzausbildung Datenschutz-Auditor (TüV Süd)
- Zusatzausbildung Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- 10 Jahre klinische Erfahrung
- 20 Jahre IT im Krankenhäusern
- 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.

AGENDA

Worum geht es

- Abgrenzung
- Patientendaten sind geschützt
- Grundanforderungen im Datenschutz
- Weitergehende Anforderungen
- Anforderungen außerhalb des Datenschutzes

ABGRENZUNG

Es gibt (so gut wie keine) „telemedizinische“ Gesetzgebung

- Ziviles Recht, Strafrecht usw. gilt generell
- D.h. Es gibt kein spezielles telemedizinisches Datenschutzrecht, Haftungsrecht usw.
- Aber: es gibt spezielle Regelungen wie z.B.
  - Teleradiologie nach Röntgenverordnung (§2 Ziff. 24, §3 Abs. 4, §4 Abs. 4 RöV)
  - Verbot der ausschließlichen telemedizinischen Behandlung (§7 Abs. 4 MBO-Ä)
  - Rahmenvereinbarung für telemedizinische Leistungen entsprechend § 87 Abs. 2a Satz 8 SGB V

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz

Arbeitsrecht

Datenschutzrecht

Standes-, Berufsrecht

Strafrecht

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz: Arbeitsrecht

- Angestellte Chefärztinnen, Oberärzte, Pflegepersonal, ...
- Gesetz gegen den unlauteren Wettbewerb (UWG)
- § 17 Verrat von Geschäfts- und Betriebsgeheimnissen
  - „Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis..."
    Patientendaten in einer Arztpraxis/Krankenhaus = Geschäfts- oder Betriebsgeheimnis
  - „...während der Geltungsdauer des Dienstverhältnisses
  - unbefugt
  - an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, ..."
    „zugunsten eines Dritten" = z.B. Krankheitsregister, Pharmafirmen, ...
- Kernaussage: „unbefugt"
  - Befugnis kommt vom Arbeitgeber

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz: Standesrecht

- Muster-Berufsordnung für Ärzte/Ärztinnen (bzw. die jeweilige Landesordnung)
- §9 MBO-Ä: Schweigepflicht
  - Abs. 1: „… über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist …“
  - Abs. 2: „ Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist.“
  - Abs. 4: „Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist.“
- Kernaussage: „unbefugt“
  - Wissen kommt aus der ärztlichen Tätigkeit
  - Befugnis kommt vom Patienten: Befreiung von Schweigepflicht liegt vor oder ist anzunehmen

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz: Strafrecht

- §203 StGB „Verletzung von Privatgeheimnissen“
  - Abs. 1: „Wer unbefugt ein fremdes Geheimnis ... offenbart, das ihm als Arzt ... anvertraut worden oder sonst bekanntgeworden ist, ...“
- Kernaussage: „unbefugt“, „offenbart“
  - Wissen kommt aus der ärztlichen Tätigkeit
  - Befugnis kommt vom Patienten: Befreiung von Schweigepflicht liegt vor
  - Offenbart: bewusst weitergegeben oder unzulänglich vor Kenntnisnahme durch Dritte geschützt

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz: Datenschutzrecht

- **Bundesrecht:**
  - BDSG
  - Sozialgesetzbücher
  - Telemediengesetz
  - ...
- **Landesrecht**
  - Landesdatenschutzgesetze
  - Krankenhausgesetze
  - Heilberufsgesetz
- **Kirchenrecht**
  - Evangelische Kirche
  - Katholische Kirche

- **Rechtmäßigkeit der Datenverarbeitung**
  - Gesetzliche Grundlagen
  - Einwilligung
- **Grundsatz der Zweckbindung**
- **Grundsatz der Erforderlichkeit**
- **Grundsatz der Datenvermeidung und Datensparsamkeit**
- **Grundsatz der Transparenz**
- **Grundsatz der klaren Verantwortlichkeiten**
- **Grundsatz der Kontrolle**
- **Grundsatz der Gewährleistung der Betroffenenrechte**
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- **Nutzung pseudonymisierter oder anonymisierter Daten**
- **Verpflichtung zum Schutz der Daten**

PATIENTENDATEN SIND GESCHÜTZT

Vierfacher Schutz: Datenschutzrecht (ab 25. Mai 2018)

- **Europarecht**
  - **Datenschutz-Grundverordnung**
- **Bundesrecht:**
  - „DS-GVO-Umsetzungsgesetz“
  - Sozialgesetzbücher (?)
  - Telemediengesetz (?)
  - ...
- **Landesrecht**
  - Landesdatenschutzgesetze (?)
  - Krankenhausgesetze (?)
  - Heilberufsgesetz
- **Kirchenrecht**
  - Evangelische Kirche (?)
  - Katholische Kirche (?)

- **Rechtmäßigkeit der Datenverarbeitung**
  - Gesetzliche Grundlagen
  - Einwilligung
- **Grundsatz der Zweckbindung**
- **Grundsatz der Erforderlichkeit**
- **Grundsatz der Datenvermeidung und Datensparsamkeit**
- **Grundsatz der Transparenz**
- **Grundsatz der klaren Verantwortlichkeiten**
- **Grundsatz der Kontrolle**
- **Grundsatz der Gewährleistung der Betroffenenrechte**
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- **Nutzung pseudonymisierter oder anonymisierter Daten**
- **Verpflichtung zum Schutz der Daten**

GRUNDANFORDERUNGEN IM DATENSCHUTZ

Verbot mit Erlaubnisvorbehalt

- Ist eine Verarbeitung nicht ausdrücklich erlaubt, so ist sie verboten
- Wann ist eine Verarbeitung erlaubt?
  - Gesetzliche Erlaubnis, z.B.
    - Sozialgesetzbuch
    - Handelsgesetzbuch (HGB)
    - Telemediengesetz (TMG)
  - Einwilligung des Betroffenen
    - Hinweis: nur möglich, wenn Gesetz Verarbeitung nicht abschließend regelt (z.B. Sozialdaten)

GRUNDANFORDERUNGEN IM DATENSCHUTZ

Erforderlichkeit und Minimalisierung

- Erforderlichkeit ist dann gegeben, wenn ohne die Daten die Aufgabe gar nicht oder zumindest nicht vollständig erfüllt werden kann (als conditio sine qua non).
- Erforderlichkeit ist schon dann gegeben, wenn Daten zur Erreichung des Zwecks objektiv geeignet sind und im Verhältnis zum Zweck auch angemessen erscheinen (Dies schließt auf jeden Fall eine Vorratsspeicherung oder die Speicherung von Hintergrundinformationen aus).
- Ziel:
  - so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
  - „Es ist einfacher so“ führt nicht zu einer Erfordernis und widerspricht dem Gebot der Datenvermeidung und Datensparsamkeit

GRUNDANFORDERUNGEN IM DATENSCHUTZ

Unabdingbare Rechte des Betroffenen

- Recht auf Auskunft
  - Umfang der gespeicherten Daten
  - Herkunft und Empfänger der Daten
  - Zweck der Speicherung
  - Adressat bei regelmäßiger Datenübermittlung
  - Grundsätzlich schriftlich und kostenfrei
- Recht auf Berichtigung, Sperrung und Löschung
  - Löschung bei unrichtiger Speicherung
  - Löschung, wenn nicht mehr erforderlich
- Recht auf Benachrichtigung
  - bei erstmaliger Speicherung
  - Art der Daten
- Recht auf Widerspruch
- Recht auf Schadensersatz

GRUNDANFORDERUNGEN IM DATENSCHUTZ

Unabdingbare Rechte des Betroffenen (ab 25. Mai 2018)

- **Recht auf Auskunft**
  - Umfang der gespeicherten Daten
  - Herkunft und Empfänger der Daten
  - Zweck der Speicherung
  - Dauer der Speicherung
  - Adressat bei regelmäßiger Datenübermittlung
  - Grundsätzlich schriftlich und kostenfrei
- **Recht auf Berichtigung, Sperrung und Löschung**
  - Löschung bei unrichtiger Speicherung
  - Löschung, wenn nicht mehr erforderlich
- **Recht auf Benachrichtigung**
  - bei erstmaliger Speicherung
  - bei Zweckänderung
  - bei Entsperrung
  - Art der Daten
- **Recht auf Widerspruch**
- **Recht auf Schadensersatz**
- **Recht auf Datenübertragbarkeit**

GRUNDANFORDERUNGEN IM DATENSCHUTZ

Zusätzlich ab 25. Mai 2018: Beachtung/Einhaltung Art. 5 DS-GVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicher(-dauer-)begrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

WEITERGEHENDE ANFORDERUNGEN

Sichere Zuordnung: elektronische Signatur

- Von wem stammt das Dokument? Wurde es geändert? Kann ich dem Dokument „vertrauen“?
- Verwendung von Daten = es haftet immer der Tätige
- Daher
  - Nachweis, von wem ein Dokument stammt, unabdingbar
  - Nachweis, ob ein Dokument geändert wurde, unabdingbar
- Lösung: Verwendung digitaler Signaturen

WEITERGEHENDE ANFORDERUNGEN

Nachweis, wer wann auf welche Daten aus welchen Gründen zugriff

- Berechtigungskonzept notwendig
  - DIN EN ISO 22600-1 „Privilegienmanagement und Zugriffssteuerung“, Teil 1: Übersicht und Policy-Management
  - DIN EN ISO 22600-2 „Privilegienmanagement und Zugriffssteuerung“, Teil 2: Formale Modelle
  - DIN EN ISO 22600-3 „Privilegienmanagement und Zugriffssteuerung“, - Teil 3: Implementierungen
- Protokollierungskonzept notwendig
  - DIN EN ISO 27789 „Audit-Trails für elektronische Gesundheitsakten“
- (Löschkonzept notwendig)
  - DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“

WEITERGEHENDE ANFORDERUNGEN

Abschätzung des Risikos des Betroffenen

- Pflicht ab 25. Mai 2018
- „Datenschutzfolgenabschätzung“
  - ISO/IEC DIS 29134 (Entwurf) „Privacy impact assessment – Guidelines“
  - Fernwartung
    - ISO/TR 11633-1:2009-11 "Medizinische Informatik - Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen - Teil 1: Anforderungen und Risikoanalyse"
    - ISO/TR 11633-2:2009-11 "Medizinische Informatik - Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen - Teil 2: Implementierung eines ISMS"

WEITERGEHENDE ANFORDERUNGEN

Schutz der Daten

- Stand heute
  - Technisch-organisatorische Maßnahmen (Anlage zu § 9 Satz 1 BDSG)
- Ab 25. Mai 2018: Art. 32 DS-GVO „Sicherheit der Verarbeitung“
  - Stand der Technik unter Berücksichtigung
    - Pseudonymisierung und Verschlüsselung personenbezogener Daten
    - Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
    - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
    - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
  - Gesetze außerhalb des medizinischen Focus können auch auf Gesundheitsdienstleister zutreffen

WEITERGEHENDE ANFORDERUNGEN

Umsetzung von IT-Sicherheit

- Gesetze außerhalb des medizinischen Focus können auch auf Gesundheitsdienstleister zutreffen
  - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
    - Zielsetzung: Unternehmensführungsmethoden zu installieren, die ermöglichen Entwicklungen frühzeitig zu erkennen, die den Fortbestand des Unternehmens gefährden könnten
  - Kreditwirtschaft
    - Badel II, EuroSOX, MaRisk
  - TKG, TMG
    - Schutz der Daten im Gesetz vorgeschrieben (§13 Abs. 4,7 TMG bzw. §109a TKG)
- Wirtschaftsprüfung
  - Prüfstandards (PS) vom Institut der Wirtschaftsprüfer (IDW)

    Z.B. IDW PS 30 enthält Richtlinien
    - Ziele und Umfang von IT-Systemprüfungen
    - Durchführung von IT-Systemprüfungen
    - IT-gestützte Prüfungstechniken
    - Produktdokumentation und Berichterstattung

Resultierende Risikofelder
- IT-Umfeldrisiken,
- IT-Organisationsrisiken,
- IT-Infrastrukturrisiken
- -Anwendungsrisiken
- ...

ANFORDERUNGEN AUßERHALB DES DATENSCHUTZES

Standesrechtliche Zulässigkeit

- §7 Abs, 4 MBO-Ä
  - Ärztinnen und Ärzte dürfen individuelle ärztliche Behandlung, insbesondere auch Beratung, nicht ausschließlich über Print- und Kommunikationsmedien durchführen.
  - Auch bei telemedizinischen Verfahren ist zu gewährleisten, dass eine Ärztin oder ein Arzt die Patientin oder den Patienten unmittelbar behandelt.
- §19 Abs. 1 MBO-Ä
  - Ärztinnen und Ärzte müssen die Praxis persönlich ausüben.
- Kernaussage: „ausschließlich“
- Nicht wirklich „Fernbehandlungsverbot“, z.B.
  - OVG Rheinland-Pfalz, Urt. v. 21. 01. 2003 AZ 6 A 11210/02 (teleradiologischen Betrieb einer Computertomographieanlage)
  - Hinweise und Erläuterungen zu § 7 Absatz 4 MBO-Ä der Bundesärztekamme (2015-12-11, http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/2015-12-11_Hinweise_und_Erlaeuterungen_zur_Fernbehandlung.pdf)

ANFORDERUNGEN AUßERHALB DES DATENSCHUTZES

Aufklärungspflicht

- § 630e BGB „Aufklärungspflichten“
  - Abs. 1: „Der Behandelnde ist verpflichtet, den Patienten über sämtliche für die Einwilligung wesentlichen Umstände aufzuklären.“
  - „Dazu gehören insbesondere Art, Umfang, Durchführung, zu erwartende Folgen und Risiken der Maßnahme sowie ihre Notwendigkeit, Dringlichkeit, Eignung und Erfolgsaussichten im Hinblick auf die Diagnose oder die Therapie.“
  - Abs. 2: „Die Aufklärung muss mündlich durch den Behandelnden oder durch eine Person erfolgen, die über die zur Durchführung der Maßnahme notwendige Ausbildung verfügt…“
- Kernaussagen:
  - Alle Behandelnden müssen aufklären
  - Die Aufklärung muss vollumfänglich erfolgen, z.B. auch Risiken des Internets beinhalten, wenn das Internet genutzt wird
  - Die Aufklärung muss mündlich erfolgen und wird i.d.R. die Anwesenheit voraussetzen

ANFORDERUNGEN AUßERHALB DES DATENSCHUTZES

Dokumentationspflicht

- § 630f BGB „Dokumentation der Behandlung “
  - Abs. 1: „Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen.“
  - „Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind.“
  - Abs. 2: „ Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen.“
- Kernaussagen:
  - Alle Behandelnden müssen dokumentieren
  - Die Dokumentation muss alle relevanten Punkte beinhalten, Änderungen müssen nachvollziehbar sein

ANFORDERUNGEN AUßERHALB DES DATENSCHUTZES

Medizinprodukterecht

- § 3 Abs. 1 Medizinproduktegesetz
  - Medizinprodukte sind ... , Apparate, Vorrichtungen, Software ... zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke
    - der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
    - der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
    - der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
    - der Empfängnisregelung
- Kernaussage:
  - Auch telemedinizische Produkte können Medizinprodukte sein
  - Daraus resultieren vielfältige Pflichte, z.B. bzgl. Dokumentation der Software, Rückrufmechanismen, ...

ANFORDERUNGEN AUßERHALB DES DATENSCHUTZES

Medizinischer Internetauftritt, App zur Kommunikation

- Telekommunikationsgesetz (TKG)
  - Beachtung Fernmeldegeheimnis (§§ 88-90 TKG)
  - Datenschutz (§§ 91-107 TKG)
  - Sicherheit (§§ 208-155 TKG, insbesondere 109a TKG)
- Telemediengesetz (TMG)
  - §5 TMG: Informationspflicht (Impressum)
  - Kommerziell: §6 TMG – zusätzliche Informationspflichten
    - Kommerzielles klar ersichtlich, Angebote usw. eindeutig erkennbar, ...
  - §13 TMG: datenschutzrechtliche Pflichten
    - Information, Einwilligung, TOMs zur Aufrechterhaltung des Dienstes sowie zum Schutz der persdonenbezogenen Daten
- Rundfunkstaatsvertrag (RStV)
  - §§55, 57, 58 Abs. 2 (Informationspflichten, Datenschutz, Werbung/Sponsoring)
- Ggfs. Berufsordnung beachten
  - Z.B. §27 MBO-Ä (Erlaubte Information und berufswidrige Werbung)
- Heilmittelwerbegesetz (HWG)
  - § 11 Abs. 1 HWG (Außerhalb der Fachkreise darf für Arzneimittel, Verfahren, Behandlungen, Gegenstände oder andere Mittel nicht geworben werden ...)

SPEZIALFALL TELERADIOLOGIE (NACH RÖV)

Verordnung über den Schutz vor Schäden durch Röntgenstrahle (Röntgenverordnung - RöV)

- §2 Abs. 24 RöV definiert Teleradiologie
  - „Untersuchung eines Menschen mit Röntgenstrahlung unter der Verantwortung eines Arztes nach § 24 Abs. 1 Nr. 1, der sich nicht am Ort der technischen Durchführung befindet und der mit Hilfe elektronischer Datenübertragung und Telekommunikation insbesondere zur rechtfertigenden Indikation und Befundung unmittelbar mit den Personen am Ort der technischen Durchführung in Verbindung steht."
- §3 Abs. 4 RöV beschreibt die Anforderungen bzgl. Erlaubnis zur Teleradiologie, §3 Abs. 7 RöV beschreibt die zur Unterlagen, die zur Genehmigung bereitgestellt werden müssen
  - Teleradiologie nach RöV ist genehmigungspflichtig
  - „Normale" Teleradiologie (z.B. Zweitmeinung) ist nicht geregelt
- Eine Anforderung (§3 Abs. 4 Ziff. 4 lit. c RöV)
  - die Ausrüstungen vorhanden und die Maßnahmen getroffen sind, die nach dem Stand der Technik erforderlich sind, damit die Anforderungen an den Betrieb der Röntgeneinrichtung im Rahmen freiwilliger Röntgenreihenuntersuchungen erfüllt sind

DISKUSSION