Fernwartung und anderes Outsourcing – die §203 Problematik

Dicom-Treffen 2014

Dr. Bernd Schütze

HEALTHCARE SOLUTIONS

§203 StGB

(1) Wer **unbefugt** ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs …

(3) … Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen **Gehilfen** und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.

Gehilfe im Sinne des §203

- Qualifikation nicht entscheidend
- Unmittelbar den Arzt unterstützend
- Schweigepflichtige (= Arzt) muss gegenüber dem Gehilfen weisungsberechtigt sein
  - entbehrlich, wenn sich die Zuordnung zur Funktionseinheit des Schweigepflichtigen schon erkennbar aus anderen Umständen ergibt
  - Im Krankenhaus angestellte (Bsp. Kaufmännischer Direktor) = Gehilfe
  - Externe ohne Arbeitnehmerüberlassung ≠ Gehilfe
- Berufsmäßig tätig?
  - Nebentätigkeiten?
  - Ehrenamtliche Aktivitäten?
  - Arbeitsvertrag notwendig? (Wahrscheinlich nein)

Unbefugte Offenbarung: Lösung durch Auftragsdatenverarbeitung?

- ADV-Regelung entsprechend §11 BDSG keine Offenbarungsbefugnis:

  §1 Abs. 3 BDSG

  „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

  Die **Verpflichtung zur Wahrung** gesetzlicher Geheimhaltungspflichten oder von **Berufs-** oder besonderen Amts**geheimnissen**, die nicht auf gesetzlichen Vorschriften beruhen, **bleibt unberührt**.“

Auftragsdatenverarbeitung und Landesrecht

Landesrechtliche Vorschriften zur ADV im Krankenhaus existieren in

- Baden-Württemberg (§ 48 LKHG BW)
- Bayern (Art. 27 Absatz 4 Satz 5, Absatz 6 BayKHG)
- Berlin (§24 Abs. 6 LKG)
- Bremen (§ 10 BremKHDSG)
- Hamburg (§ 9 HmbKHG)
- Hessen (§§ 11,12 HKHG i. V. m § 4 Abs. 2 letzter Satz HDSG)
- Mecklenburg-Vorpommern (§ 21 LKHG M-V)
- Nordrhein-Westfalen (7 Abs. 3 GDSG)
- Rheinland-Pfalz (§ 36 Abs. 9 LKG)
- Saarland (§ 13 Abs. 7 Saarländisches KHG)
- Sachsen (§ 33 Abs. 10 SächsKHG)
- Thüringen (§ 27b des Thüringer Krankenhausgesetzes)

Keine landesrechtlichen Vorschriften gibt es in

- Brandenburg
- Niedersachsen
- Sachsen-Anhalt
- Schleswig-Holstein

Gehilfe und ADV-Anforderung

Anforderung an einen Gehilfen	Bestandteil eines ADV-Vertrages
Berufsmäßig tätig	– Vertragsgestaltung
Ausübung der unterstützenden Tätigkeit innerhalb des beruflichen Wirkungskreises des Schweigepflichtigen	– Der Gegenstand und die Dauer des Auftrags – Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen – Die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen
Unmittelbarer Zusammenhang zwischen der Tätigkeit des Unterstützers und derjenigen des Schweigepflichtigen	– Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen – Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält

Gehilfe und ADV-Anforderung

Anforderung an einen Gehilfen	Bestandteil eines ADV-Vertrages
Es bedarf einer qualifizierten Unmittelbarkeitsbeziehung zwischen Berufsgeheimnisträger und Gehilfe	– Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält
Generelle Erfordernis eines Direktionsrechts bzw. einer effektiven Steuerungsmacht	– Die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen – Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält

Landesrecht als Offenbarungsbefugnis?

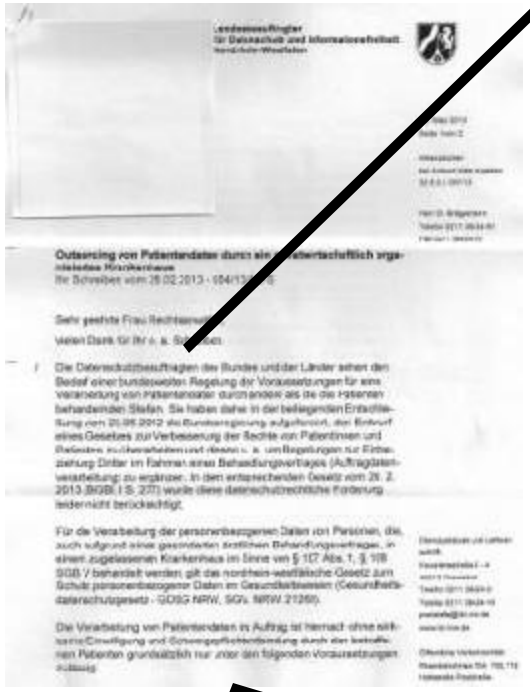
Bsp. Hessen

28. Tätigkeitsbericht des hess. DSB, 28. März 2000
8.3 Verarbeitung personenbezogener Daten im Auftrag hessischer Krankenhäuser (S. 71ff)

Für die Vergabe von Aufträgen an nicht-öffentliche Stellen werden in § 4 Abs. 3 Satz 4 HDSG weitere rechtliche Vorgaben festgelegt. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen oder Berufs- oder besondere Arztgeheimnisse noch überwiegende schutzwürdige Belange entgegen stehen. Da § 12 HKHG ausdrücklich auf die Vorschriften des Hessischen Datenschutzgesetzes verweist, steht die ärztliche Schweigepflicht einer Weitergabe der Patientendaten an einen Auftragnehmer nicht entgegen, insoweit liegt eine spezialgesetzliche Rechtsgrundlage für die Offenbarung der Patientendaten an einen Auftragnehmer vor

Landesrecht als Offenbarungsbefugnis?

Bsp. NRW (Schreiben vom 26. März 2013)



Die Datenschutzbeauftragten des Bundes und der Länder sehen den Bedarf einer bundesweiten Regelung der Voraussetzungen für eine Verarbeitung von Patientendaten durch andere als die die Patienten behandelnden Stellen. Sie haben daher in der beiliegenden Entschließung vom 23.05.2012 die Bundesregierung aufgefordert, den Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten zu überarbeiten und diesen u. a. um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragdatenverarbeitung) zu ergänzen. In dem entsprechenden Gesetz vom 20. 2. 2013 (BGBl. I S. 277) wurde diese datenschutzrechtliche Forderung leider nicht berücksichtigt.

Vor der Vergabe eines Auftrages zur Verarbeitung von Patientendaten hat sich der Auftraggeber zu vergewissern, dass beim Auftragnehmer die Wahrung der Datenschutzbestimmungen des Gesundheitsdatenschutzgesetzes und der ärztlichen Schweigepflicht sichergestellt ist.

Landesrecht als Offenbarungsbefugnis?

- Bsp. Rheinland-Pfalz
  - § 36 Abs. 9 LKG erlaubt eine Auftragsdatenverarbeitung, wenn eine § 203 StGB entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist
- Frage: Wie stellt der Auftraggeber die Wahrung der ärztlichen Schweigepflicht beim Auftragnehmer sicher?
  - I.D.R. kein Schweigerecht beim Auftragnehmer vorhanden
- Generelle Frage:
  - Kann dieses Landesrecht das strafrechtliche Bundesrecht brechen?

Aktuelle Lage

- Krankenhausarzt hat i.d.R. keinen Einfluss auf Vertragsgestaltung bzgl. Fernwartung von Systemen/Medizingeräten
- Krankenhausarzt ist aber entsprechend §203 StGB für Einhaltung ärztlicher Schweigepflicht verantwortlich
- Unklare Rechtsgrundlage:
  - Kann externer Mitarbeiter bei Fernwartung als „Gehilfe“ angesehen werden?
  - Kann ADV-Vertrag entsprechend Landesrecht als Offenbarungsbefugnis angesehen werden?

Konsequenzen für den Arzt

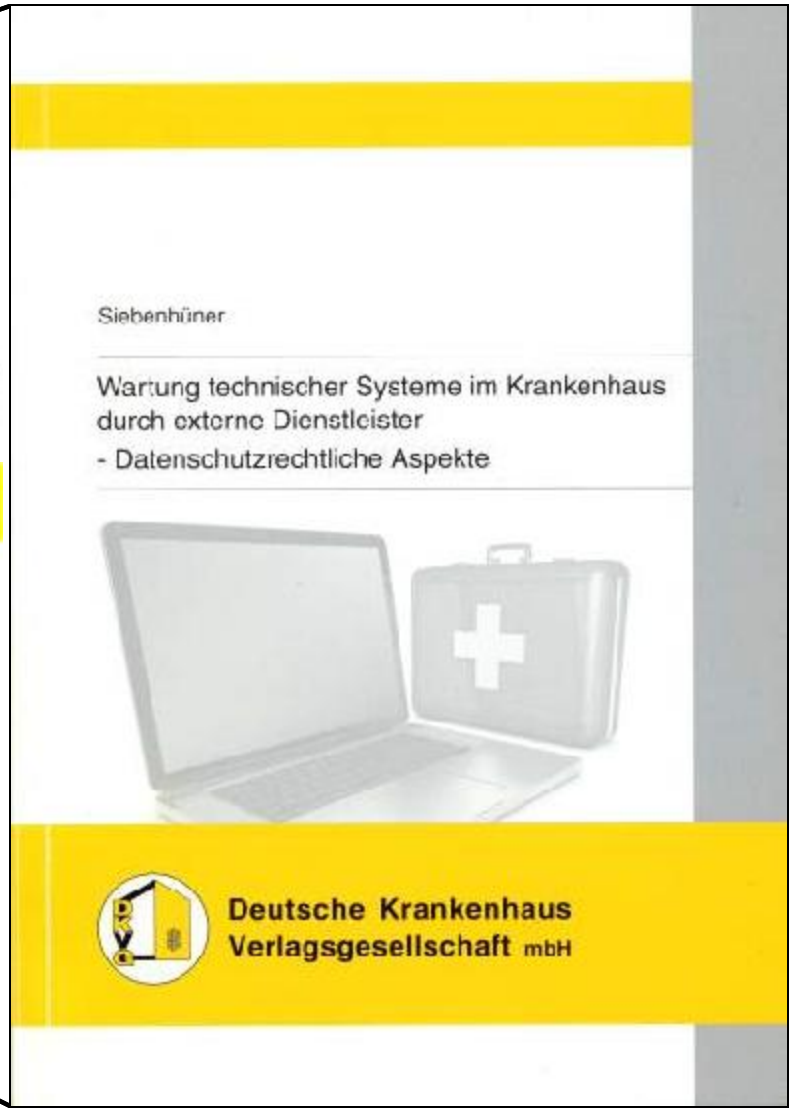
- Outsourcing von Dienstleistungen im Krankenhaus datenschutzrechtlich in den meisten Bundesländern umsetzbar
- Strafrechtlich ist Outsourcing nahezu immer mit der unbefugten Offenbarung des Arztgeheimnisses verbunden
  - Evtl. Ausnahme: Arbeitnehmerüberlassung
- Arbeitnehmerüberlassung für Krankenhaus keine Lösung
  - Personalrat/Betriebsrat Krankenhaus muss zustimmen
  - Personalrat/Betriebsrat Dienstleister muss zustimmen
  - Personal des Dienstleisters betreut i.d.R. eine Vielzahl von Krankenhäusern -> Wie viele Verträge soll Dienstleister abschließen? Wie viele das Krankenhaus?

Veröffentlichung Deutsche Krankenhaus Verlagsgesellschaft

6. Schlussbetrachtung

Nach der vorliegenden Betrachtung der Fragestellung nach der Zulässigkeit der Wartung von technischen Systemen durch externe Dienstleistungsunternehmen im Krankenhaus kann folgendes Gesamtergebnis festgehalten werden:

Lediglich die Fremdwartung von Systemen mit Klartextinformationen und pseudonymisierten Patientendaten ist aufgrund von straf- und berufsrechtlichen Bestimmungen nicht zulässig. Der Gefahr des Offenbarens kann durch den Einsatz eines Geheimhaltungsverpflichteten, welcher die Wartung autorisiert, überwacht und bei Bedarf zeitgerecht zum Schutz der Patientendaten einschreitet, erfolgreich begegnet werden. Aus Gründen der Praktikabilität sollte der Geheimhaltungsverpflichtete der betriebliche Datenschutzbeauftragte sein.



Deutsche Krankenhaus Verlagsgesellschaft mbH, 1. Auflage 2013, ISBN 978 -3-942734-49-3

Veröffentlichung Deutsche Krankenhaus Verlagsgesellschaft

Wenn die Deutsche Krankenhausgesellschaft die Fernwartung durch Hersteller als rechtswidrig ansieht,
sofern der Zugriff auf Patientendaten nicht ausgeschlossen werden kann,
wie wird dann wohl ein vom Gericht bestellter Gutachter das Geschehen beurteilen?

Deutsche Krankenhaus Verlagsgesellschaft mbH, 1. Auflage 2013, ISBN 978 -3-942734-49-3

Konsequenzen für den Arzt

- §203 StGB Antragsdelikt
  - Wird also nur auf Antrag des Betroffenen verfolgt
  - Unwahrscheinlich, dass es passiert, daher bisher geringe Praxisrelevanz
  - Bedingt durch die Veröffentlichung der Krankenhausgesellschaft kann sich dies ändern (siehe Anstieg Auskunftsersuchen nach Verabschiedung Patientenrechtegesetz
  - Bekanntermaßen existiert „Querulantentum“
- Wenn Antrag gestellt wird, Verurteilung unter derzeitiger Lage nicht unwahrscheinlich
- Ggfs. Organisationsverschulden, daher zivilrechtliche Weitergabe an Krankenhaus möglich
- Aber Worst Case Szenario: Verlust Approbation

Forderung

- Nutzung moderner IT oder von Medizingeräten nur mit Unterstützung des jeweiligen Herstellers möglich
- Fernwartung die Regel, alles andere derzeit unbezahlbar
- Bei Fernwartung kann es zur Offenbarung von Patientengeheimnissen kommen
- Verschulden eines Arztes liegt hierbei nicht vor
- Daher Anpassung der Gesetzgebung erforderlich:
  - ADV muss Offenbarungsbefugnis darstellen

Weiteres Vorgehen

- Arbeitsgruppe gebildet:
  - bvitg
  - BvD
  - GDD
  - GMDS
- Zielsetzung
  - Vorschlag zur Gesetzesänderung bzgl. §203 StGB
  - „Muster“-Vertrag für die Auftragsdatenverarbeitung
- Initiales Treffen: 10. Juli 2014

➲ Wenn jemand Kontakt zu Vertretern der Ärzteschaft hat: mehr Lobbyvertreter schaden nicht ;-)
Ggfs. bitte Kontakt mit mir aufnehmen

Ausblick

Damit niemand glaubt es wird langweilig…

- Ist der Entwurf des „IT-Sicherheitsgesetz“ bekannt?
- Kommentierung ist abgeschlossen, seitens Gesundheitswesens nur von der Bundesärztekammer kommentiert
- Einige (An-) Forderungen:
  - Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit nach dem Stand der Technik
  - Zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen sind spätestens 2 Jahre nach Inkrafttreten der Verordnung sowie anschließend mindestens alle zwei Jahre Sicherheitsaudits durch anerkannte Auditoren durchzuführen.
  - Mindestens alle 2 Jahre sind dem BSI eine Aufstellung der durchgeführten Sicherheitsaudits einschließlich der aufgedeckten Sicherheitsmängel zu übermitteln
  - Es besteht eine Meldepflicht bzgl. „erheblicher“ Sicherheitsmängel an das BSI
  - …

Vielleicht mehr im nächsten Jahr…

Ausblick

- Entwurf EU-Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit“
  „Cybersicherheitsrichtlinie“ vom 7. Februar 2013
- Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme
  „IT-Sicherheitsgesetz“ (IT-Sig) vom 5. März 2013)

Diskussion

schuetze@medizin-informatik.org

(GPG-Schlüssel auf dem Server abrufbar)