Datenschutz · Ergonomie · Mitbestimmung
www.sovt.de

Auftragsdatenverarbeitung in Krankenhäusern und anderen med. Einrichtungen

Spezialgesetzliche Erlaubnisse im Hinblick auf Standort, Trägerschaft, Rechtsform

Berlin, 25. Mai 2011

Lothar Bräutigam

Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Wer ist sovt?

Beratung zum betrieblichen Datenschutz

- Schwerpunkt: Datenschutz im Krankenhaus
- Schwerpunkt: Arbeitnehmerdatenschutz
- Externer Datenschutzbeauftragter (auch in Krankenhäusern, Reha-Kliniken)
- Entwicklung von Datenschutz-Leitfäden für Siemens medico//s und Soarian IC
- Seminare zum betrieblichen Datenschutz
- Coaching von internen Datenschutz-beauftragten
- Externer Sachverständiger für Betriebs- und Personalräte

Fritz-Glenz-Str. 3
64297 Darmstadt

Tel. (06151) 62 60 2
Fax (06151) 62 60 6
eMail: info@sovt.de
Internet: www.sovt.de

Überblick

1. **Outsourcing – praktische Beispiele**
2. Datenschutzrechtliche Einordnung
3. Lösungsmöglichkeiten

Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Outsourcing von Dienstleistungen

... i.V.m. der Verarbeitung von Patientendaten

- Schreiben von Arztbriefe (externes Schreibbüro)
- Externe Digitalisierung der Patientenakten
- Verwaltung des Patientenaktenarchivs durch externen Dienstleister
- Abholung und Vernichtung von Patientenakten
- Betriebs der IT-Systeme eines MVZ durch das angeschlossene KH
- Fernwartung des KIS (bzw. der Praxissoftware)

Outsourcing von Dienstleistungen

- Mehrmonatige Beschäftigung eines Medizincontrollers als Mitarbeiter einer ext. Firma
- Besetzung der Pforte mit Personal einer Security-Firma
- Abrechnung ambulanter oder wahlärztlicher Chefarztbehandlungen durch berufsständische Verrechnungsstellen
- Abrechnung ambulanter Notfallbehandlungen des Kranken-hauses (gegenüber der KV) über externe Dienstleister
- Eintreiben von Forderungen über Inkassobüros
- Outsourcing des Labors
- Physikalische Therapie durch ext. Dienstleister im Krankenhaus

Fragen

- **Datenschutzrechtliche Einordnung:**
  - Datenverarbeitung im Auftrag?
  - Übermittlung („Funktionsübertragung“)?
  - oder was sonst?
- **Ist das datenschutzrechtlich zulässig?**
- **Unter welchen Voraussetzungen oder Auflagen?**
- **Unterschiede für verschiedene med. Einrichtungen?**

Überblick

1. Outsourcing – praktische Beispiele
2. **Datenschutzrechtliche Einordnung**
3. Lösungsmöglichkeiten

Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Abgrenzungen

Die folgenden Fälle müssen unterschieden werden:

- **Datenverarbeitung im Auftrag:**
  - Auftraggeber bleibt verantwortlich
  - Auftragnehmer erhält Weisungen, keine eigenen Entscheidungsspielräume
  - keine Verwendung der Daten durch Auftragnehmer zu eigenen Zwecken
- **Übermittlung („Funktionsübertragung“)**
  - Auftragnehmer verwendet Daten zu eigenen Zwecken
  - nach eigenen Entscheidungen
  - Auftragnehmer ist Dritter, Erlaubnistatbestand erforderlich
- **Mit- oder Nachbehandlung**
  - Empfänger ist eine med. Einrichtung, die im gleichen Behandlungsfall tätig wird (z.B. per Überweisung)
  - Empfänger ist Dritter, Übermittlung liegt vor
  - Konkludente Einwilligung des Patienten nach Information ausreichend (§ 9 Abs. 4 MBO-Ä)

Ärztliche Schweigepflicht

§ 9 MBO-Ä regelt die ärztliche Schweigepflicht:

(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist - auch über den Tod des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(2) Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutz eines höherrangiges Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht des Arztes einschränken, soll der Arzt den Patienten darüber unterrichten.

(3) Der Arzt hat seine Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

(4) Wenn mehrere Ärzte gleichzeitig oder nacheinander den selben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist.

Datenverarbeitung im Auftrag

§ 11 BDSG:

- Privilegierte Verarbeitung: Auftragnehmer ist kein Dritter
- Schriftliche Auftragserteilung mit Weisungen zur Umsetzung des Datenschutzes
- **seit 2009:** Liste mit verbindlichen Regelungspunkten (in § 11 Abs. 2)
- Auftraggeber muss die Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer prüfen, vor Beginn der Auftrags-DV und danach regelmäßig.
- **seit 2009:** Ergebnis ist zu dokumentieren.
- **seit 2009:** Bußgeld bis zu 50.000 € bei Nichteinhaltung der Vorgaben
  - zur Auftragserteilung und
  - zur Prüfung der techn. + org. Maßnahmen beim Aufragnehmer vor Beginn der Auftrags-DV.

Datenverarbeitung im Auftrag (§ 11 BDSG)

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

(...) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

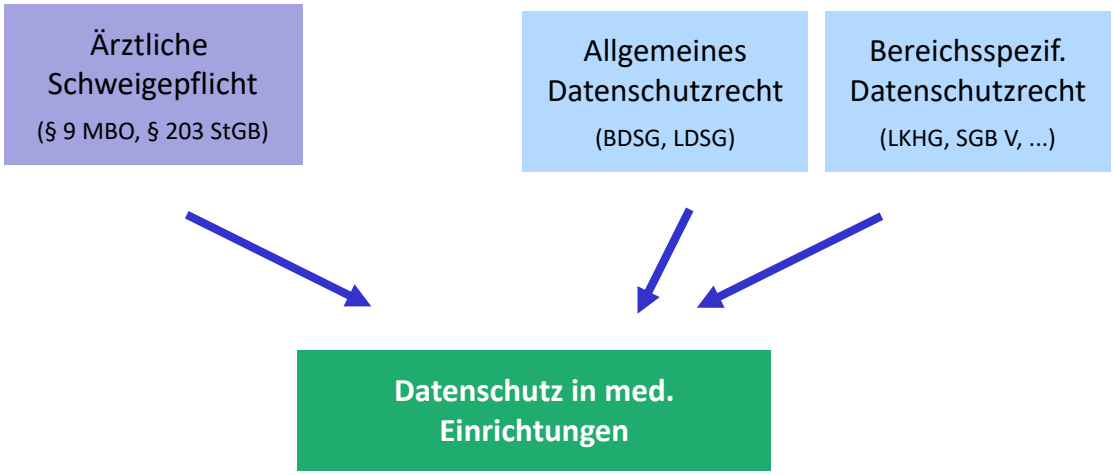
Datenverarbeitung im Auftrag

Vertragsgestaltung:

- Gegenstand des Vertrags: Leistungen des Auftragnehmers
- Definition der Weisungs- und Kontrollrechte des Auftraggebers
  - Zugangsrecht für Beauftragte des Auftraggebers (bDSB, ggf. auch BR/PR)
- Sanktionsregelungen bei Missachtung vertraglicher Pflichten
  - Mitteilungspflichten des Auftragnehmers
  - Sonderkündigungsrecht
- Technische und org. Maß-nahmen beim Auftragnehmer, besonders:
  - Zugriffsrechte
  - Protokollierung
  - Löschung, Vernichtung v. Unterlagen, Datenträgern
  - Trennung von anderen Datenbeständen , (...)
- Umfang der Verfahrensdoku-mentation
- Unterauftragsverhältnisse
- Datensicherung

An die neue Rechtslage angepasster Mustervertrag beim Dezernat Datenschutz des Regierungspräsidiums Darmstadt (unter www.rp-darmstadt.hessen.de)

Datenschutz in med. Einrichtungen



- kein einheitliches Datenschutzrecht in med. Einrichtungen !
- abhängig u.a. von Rechtsform, Träger, Bundesland
- Kirchen haben eigene Rechtsetzungskompetenz (KDO, DSG-EKD)
- unterschiedliche Verantwortlichkeiten für Datenschutz und ärztliche Schweigepflicht

(Ärztliche) Schweigepflicht

➔ **(Ärztliche) Schweigepflicht** (Patientengeheimnis)

Verbot der *unbefugten* Offenbarung ohne Entbindung durch den Patienten oder eine gesetzliche Regelung

- **§ 203 StGB:**
  - Sanktionierung der Verletzung berufsrechtlicher Geheimnisse
  - Enge Ausnahmeregelung
  - Geldstrafe oder Freiheitsstrafe bis zu 2 Jahre
- **tlw. in Berufsordnungen weiter geregelt**
  - z.B. Berufsordnungen der Landesärztekammern
- **§ 53 StPO (bzw. § 383 ZPO):**
  - Zeugnisverweigerungsrecht des Schweigepflichtigen vor Gericht
- **§ 97 (1),(2) StPO:**
  - Beschlagnahmeschutz für Krankenunterlagen

Ärztliche Schweigepflicht

Strafgesetzbuch (StGB):

§ 203 Verletzung von Privatgeheimnissen

(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 andere Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, (...)

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (...)

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

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Ärztliche Schweigepflicht

§ 9 MBO-Ä regelt die ärztliche Schweigepflicht:

(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist - auch über den Tod des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(2) Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutz eines höherrangiges Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht des Arztes einschränken, soll der Arzt den Patienten darüber unterrichten.

(3) Der Arzt hat seine Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

(4) Wenn mehrere Ärzte gleichzeitig oder nacheinander den selben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist.

Fazit

- **Auftrags-DV in med. Einrichtungen ist *datenschutz-rechtlich* kein Problem**
- **Problem: Häufig liegt eine unbefugte Offenbarung von Patientendaten gegenüber dem Dienstleister vor**
  - die praktische Möglichkeit, Patientendaten einzusehen, erfüllt bereits den Tatbestand der unbefugten Offenbarung
  - Es liegt ein Straftatbestand vor !
  - Ausnahme: Mit- und Nachbehandlung

Datenschutz · Ergonomie · Mitbestimmung
www.sovt.de

Überblick

1. Outsourcing – praktische Beispiele
2. Datenschutzrechtliche Einordnung
3. **Lösungsmöglichkeiten**

Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

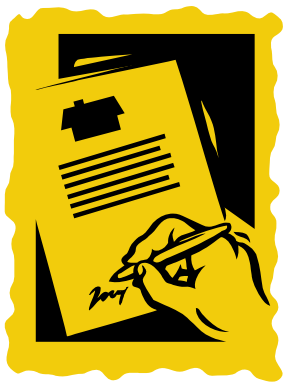
Lösungsmöglichkeiten

- Offenbarung von Patientendaten vermeiden
  - verschlüsselte Datenspeicherung
  - anomymisierte Datenübertragung
- Einwilligung des Patienten (bzw. Schweigepflichtsentbindung)
  - ausdrücklich, schriftlich
  - ggf. auch konkludente Einwilligung
  - häufig praktisch nicht machbar
- **Offenbarungsbefugnis durch Rechtsvorschrift**
  - z.B. Landeskrankenhausgesetze
  - für Arztpraxen, MVZ, Apotheken, Labore etc.: ---

Zulässigkeit durch Einwilligung

Einwilligung des Betroffenen

1. als Rechtsgrundlage für Erhebung, Verarbeitung und Nutzung gemäß BDSG / LDSG oder
2. zur Entbindung des Arztes von der Schweigepflicht (bei Übermittlungen)



Anforderungen:

- Freiwilligkeit (echte Wahl- und Entscheidungsfreiheit)
- Informierte Einwilligung: Information des Betroffenen über Verwendungs-zweck, Empfänger, Datenarten etc.
- Einwilligung im Einzelfall (keine pauschale Einwilligung im Rahmen des Aufnahmeformulars)
- Nach BDSG/LDSG: Grundsätzlich in Schriftform. Mögliche Ausnahmen:
  - Lebensbedrohliche Situation
  - Patient nicht ansprechbar
- Nach § 203 StGB: auch mündliche, auch konkludente Entbindung von der Schweigepflicht tlw. möglich

Konkludente und mutmaßliche Einwilligung

- Einwilligung zur Offenbarung muss grundsätzlich **ausdrücklich** erfolgen: mündlich oder schriftlich
  - keine Einwilligung nach Datenschutzrecht
- in med. Einrichtungen auch relevant: **konkludente Einwilligung**
  - durch schlüssiges oder stillschweigendes Handeln
  - Voraussetzung: Information des Patienten bzw. er muss mit damit rechnen können (z.B. Informationsweitergabe im Krankenhaus)
  - Beispiel: Überweisung an anderen Arzt oder andere Fachabteilung, wenn der Patient nach entsprechender Information nicht widerspricht (§ 9 Abs. 4 MBO-Ä)

Offenbarungsbefugnis durch Rechtsvorschrift

- Erforderlich: *bereichsspezifische* Rechtsgrundlage
- **Prüfen: Gibt es eine bereichsspezifische Erlaubnis für die DV im Auftrag in medizinischen Einrichtungen?**
- Nicht möglich: Bundes- oder Landesdatenschutzgesetze
- Möglich: Landeskrankenhausgesetze
  - z.B. § 48 LKG-BW
  - z.B. § 7 GDSG NRW
  - z.B. § 27b ThürKHG
  - z.B. Art. 27 Abs. 4, 6 BayKrG
  - z.B. § 7 PatDSO (kath. KH)

Datenverarbeitung im Auftrag (automatisiert)

- Landeskrankenhausgesetz Bayern:
  - Bei Behandlungsdaten nur durch anderes Krankenhaus (Art. 27 Abs. 4)
  - Bei Daten zur verwaltungsge-mäßen Abwicklung möglich, sofern bes. Schutzmaßnahmen gemäß Art. 27 Abs. 6 eingehalten werden
- Thüringer Krankenhausgesetz:
  - nur ausnahmsweise außerhalb des Krankenhauses zulässig, wenn erheblicher Kostenvorteil Einhaltung einer § 203 entspre-chenden Schweigepflicht und Meldung gegenüber Aufsichts-behörde (§ 27 b)
- GDSG NRW:
  - DV im Auftrag außerhalb des KH nur, wenn erheblich kosten-günstiger und
  - Sicherstellung von § 203 StGB beim Auftragnehmer und
  - Verarbeitung in getrennten Dateien und
  - Auftragnehmer unterwirft sich Kontrolle des LDI NRW (§ 7)
- Schleswig-Holstein, Niedersachsen, Sachsen-Anhalt:
  - keine Regelungen zur DV im Auftrag im Landeskranken-hausgesetz

Datenverarbeitung im Auftrag (automatisiert)

- Landeskrankenhausgesetz BW:
  - nach § 48 nur durch anderes KH oder Rechenzentrum
  - Bei Rechenzentrum:
    - Benachrichtigung der zustän-digen Aufsichtsbehörden
    - Auftragnehmer muss Mitar-beitern eine § 203 StGB ent-sprechende Schweigepflicht auferlegen
    - schriftliche Festlegung der erforderlichen Datenschutz-maßnahmen
- Hess. Krankenhausgesetz:
  - Nach § 12 (1) HKG grundsätzlich möglich
- KDO und Ordnung zum Schutz von Patientendaten in kath. KH
  (abweichend in versch. Bistümern):
  - nur möglich, wenn die Einhal-tung der geltenden Datenschutz-bestimmungen und der Geheim-haltungspflichten nach § 203 StGB gewährleistet ist.

    (Bistümer Limburg, Mainz, Speyer, Trier sowie norddt. Bistümer)
- DSVO zum DSG-EKD
  (ev. Kirche Westfalen, Rheinland, Lippe)
  - Nach § 38 (6) nur möglich, wenn die Einhaltung der geltenden Datenschutzbestimmungen und der Geheimhaltungspflichten nach § 203 StGB gewährleistet ist.

Fernwartung

- nach § 11 Abs. 5 BDSG **wie Datenverarbeitung im Auftrag**
- Problem in med. Einrichtungen: Mit der Fernwartung ist aufgrund umfassender Zugriffsrechte eine **Offenbarung von Patientendaten** verbunden
- Als Befugnis wäre eine **Rechtsgrundlage** oder die **Einwilligung** der Patienten erforderlich
  - in Krankenhäusern: teilweise möglich durch Landeskrankenhausgesetz (Erlaubnis zur DV im Auftrag)
  - in Arztpraxen und vielen anderen med. Einrichtungen: keine Erlaubnis durch Rechtsvorschrift

Fernwartung

Praktische Umsetzung einer rechtskonformen Fernwartung (Empfehlungen der Aufsichtsbehörden):

- keine automatische Einwahl ins KIS für Fernwartungsfirma, sondern
- nur nach expliziter Freischaltung durch KH-Mitarbeiter
- möglichst: Begrenzung der Zugriffsrechte der Fernwartungsfirma (ohne Zugriff auf Patientendaten)
- Beaufsichtigung aller Zugriffe seitens der Wartungsfirma durch KH-Mitarbeiter am Bildschirm, ggf. Trennung des Systemzugangs
- Revisionssichere Protokollierung aller Verarbeitungs- und Nutzungsvorgänge im Rahmen der Fernwartung (auf Seiten des Krankenhauses)

Keine Lösungsmöglichkeiten

- Verpflichtung des Auftragnehmers auf die Schweigepflicht
  - Ausnahme: über Verpflichtungsgesetz (nur für öffentliche Stellen möglich)
- Flucht in die Funktionsübertragung statt Auftrags-DV
  - ➔ Unbefugte Offenbarung
- Externer Dienstleister als „berufsmäßig tätige Gehilfen“
  - ➔ nicht möglich bei Mitarbeitern anderer Unternehmen, da keine effektive Weisungsbefugnis möglich
- Annahme einer konkludenten oder mutmaßlichen Einwilligung der Patienten
- Wegducken, aussitzen (→ Straftatbestand)

Datenschutz · Ergonomie · Mitbestimmung
www.sovt.de

Vielen Dank !

Diskussion

Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de