

Annette Hergeth

Rechtliche Anforderungen an das IT-Outsourcing im Gesundheitswesen



INHALTSVERZEICHNIS

1. Teil: Einleitung	15
2. Teil: IT-Outsourcing	17
I. Definitionen	17
1. Informationstechnik	17
2. Outsourcing	17
3. IT-Outsourcing	18
II. Gründe für Outsourcing	18
1. Konzentration auf das Kerngeschäft	19
2. Know-how des Outsourcinganbieters	19
3. Kosteneinsparung	19
4. Weitere Gründe	20
III. Gründe gegen Outsourcing	20
1. Verlust von Gestaltungsspielraum und von Know-how	21
2. Abhängigkeit vom Anbieter	21
3. Zusätzlicher Kontrollaufwand und Personalumstrukturierung	21
IV. Outsourcingformen	22
1. Umfang der ausgelagerten IT-Leistung	22
a. Partielles Outsourcing, Full Outsourcing, Geschäftsprozess-Outsourcing	22
b. Personalübergang, Asset-Transfer	23
2. Gesellschafts- und vertragsrechtliche Struktur des Outsourcing	23
a. Externes Outsourcing	23
b. Internes Outsourcing und Konzern-Outsourcing	24
V. Rechtliche Gestaltungsmöglichkeiten der Datenverarbeitung bei einem Outsourcing	24
1. Datenverarbeitung im Auftrag gemäß § 11 BDSG	24
a. Vertragsform	25
b. Pflichten des Auftragnehmers	25
c. Pflichten des Auftraggebers	25
2. Funktionsübertragung	26
a. Abgrenzung Funktionsübertragung und Datenverarbeitung im Auftrag	26
b. Pflichten des Outsourcinganbieters und des Outsourcingkunden	27
c. Datenschutzrechtliche Gestattung der Übermittlung	27

VI. Bedeutung des IT-Outsourcing im Gesundheitswesen	27
1. Patientenperspektive	28
2. Perspektive von Arztpraxis bzw. Krankenhaus	29
3. Typische Formen des Outsourcing im Gesundheitswesen	29
a. Klassisches Outsourcing	29
b. Joint-Venture	30
c. Konzern-Outsourcing	30
3. Teil: Rechtliche Anforderungen an den Schutz von Patientendaten	31
I. Dokumentationspflicht	32
1. Rechtsgrundlage	32
2. Zweck der Dokumentation	33
a. Therapiesicherung	33
b. Rechenschaftslegung	33
c. Beweissicherung	34
3. Archivierungsdauer	34
4. Dokumentation in digitaler Form	35
5. Dokumentation im Zivil- und Strafprozess	35
a. Dokumentation in Papierform	35
b. Dokumentation in digitaler Form mit qualifizierter Signatur	36
c. Dokumentation in digitaler Form ohne qualifizierte Signatur	36
II. Ärztliche Schweigepflicht	37
1. Rechtliche Grundlagen der ärztlichen Schweigepflicht	38
a. Ständesrechtliche Vorgaben	38
b. Zivilrechtliche Vorgaben	38
c. Strafrechtliche Vorgaben	38
2. Inhalt und Umfang der ärztlichen Schweigepflicht nach § 203 StGB	39
a. Tatbestand	39
aa. Normadressaten	40
bb. Geheimnis	40
cc. Anvertraut oder bekannt geworden	41
dd. Offenbaren	42
ee. Unbefugt	43
b. Rechtswidrigkeit	46
aa. Mutmaßliche Einwilligung	46
bb. Notstand und Wahrnehmung berechtigter Interessen	46
cc. Gesetzliche Offenbarungspflichten	47
3. Rechtsfolgen bei Verletzung der ärztlichen Schweigepflicht	48
a. Ständesrechtlich	48
b. Zivilrechtlich	48
c. Strafrechtlich	48

III. Ärztliche Schweigerecht und Beschlagnahmeverbot	48
1. Regelungszweck	49
2. Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 3 StPO	49
3. Zeugnisverweigerungsrecht nach § 383 Abs. 1 Nr. 6 ZPO	50
4. Beschlagnahmeverbot nach § 97 StPO	50
IV. Datenschutz bei Patientendaten	51
1. Rechtliche Grundlagen des Datenschutzes	52
a. Europarechtliche Vorgaben	52
b. Verfassungsrechtliche Vorgaben	52
c. Bundesdatenschutzgesetz, Landesdatenschutzgesetze, Landeskrankenhausgesetze	53
aa. Für Arztpraxen anzuwendende Datenschutznormen	54
bb. Für Krankenhäuser des Bundes anzuwendende Datenschutznormen	54
cc. Für Krankenhäuser der Länder anzuwendende Datenschutznormen	57
dd. Für private Krankenhäuser anzuwendende Datenschutznormen	58
ee. Für Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften anzuwendende Datenschutznormen	59
ff. Sonstige Voraussetzung für die Anwendbarkeit der Datenschutzgesetze	60
V. Verhältnis von Schweigepflicht zu Datenschutz	60
4. Teil: Zulässigkeit des IT-Outsourcing im Gesundheitswesen	63
I. IT-Outsourcing und Dokumentationspflicht	63
1. Regelungen zur Form der Dokumentation	63
2. Anforderungen an die digitale Dokumentation	64
a. Grundsatz der Ordnungsmäßigkeit aus dem Handels- und Steuerrecht	64
b. Datenschutzrechtliche Sicherungsmaßnahmen	65
3. Erreichen der Dokumentationszwecke	65
4. Digitale Dokumentation und Langzeitarchivierung	67
a. Reproduzierbarkeit der Daten	68
b. Digitale Signatur	68
5. Ergebnis	69
II. IT-Outsourcing und ärztliche Schweigepflicht	70
1. Zulässigkeit der Digitalisierung der Daten	70
a. Tatbestand	70

aa. Dritter	71
bb. Mitteilen	73
cc. Sonstige Tatbestandsmerkmale	74
b. Rechtswidrigkeit	74
c. Schuld	76
d. Ergebnis	76
2. Zulässigkeit der Übertragung der Daten über Netze	77
3. Zulässigkeit der Speicherung in einer externen Einrichtung	78
4. Zulässigkeit der Wartung	79
5. Konsequenzen für den Arzt bei unbefugten Zugriffen	82
6. Ergebnis	83
III. IT-Outsourcing und das Beschlagnahmeverbot	84
1. Beschlagnahmefreiheit bei externer Speicherung	84
2. Beschlagnahme während der Datenübermittlung	85
a. Tatbestand des § 100 a StPO	85
b. Einschränkende Auslegung	86
aa. Historische Auslegung	86
bb. Systematische Auslegung	87
3. Ergebnis	89
IV. IT-Outsourcing und Datenschutzrecht	89
1. Externe Archivierung der Patientendaten von Arztpraxen	89
a. Zulässigkeit der Übermittlung und Speicherung	90
b. Zulässigkeit der Auftragsdatenverarbeitung	90
c. Ergebnis	91
2. Externe Archivierung der Patientendaten von Krankenhäusern am Beispiel von Sachsen und Bayern	91
a. Sachsen	91
b. Bayern	92
3. Besondere Anforderungen an die Datenanonymisierung und Datenverschlüsselung bei externer Archivierung	93
V. Im Zusammenhang stehende Rechtsprechung	93
VI. Ergebnis	95
5. Teil: Rechtliche Anforderungen an die technische Datensicherheit und die Befugnis zum Datenzugriff	97
I. Datensicherheit	98
1. Die Regelungen der Anlage zu § 9 BDSG	98
2. Praktische Umsetzung der Anforderungen in der Anlage zu § 9 BDSG	99

a. Kryptographie	100
b. Digitale Signatur	101
c. Firewall	102
d. Dokumentation und Protokollierung	102
e. Physische Abschottung	103
f. Backup-Systeme	103
3. Übertragung der Daten über Internet, Standleitung, Intranet und WLAN	104
4. Insolvenz des Outsourcinganbieters	105
5. Ergebnis	106
II. Befugnis zum Datenzugriff	106
1. Komponenten eines Zugriffskontrollsystems	107
a. Identifikation und Authentifikation	107
b. Autorisierung	109
c. Autorisation	109
d. Protokollierung und Auswertung	109
e. Reaktionskomponente	109
f. Rechtespeicher	109
2. Grundmethoden der Zugriffsregelungen	109
a. Offenes System	110
b. Geschlossenes System	110
c. Benutzerbestimmte Zugriffskontrollansätze	110
d. Systembestimmte Zugriffskontrollansätze	111
e. Rollenbasierte Zugriffskontrollansätze	111
3. Stufen von Zugriffsrechten	112
4. Verantwortlichkeit für die Vergabe der Zugriffsrechte	114
5. Ergebnis	114
6. Teil: Rechtliche Würdigung eines durchgeführten IT-Outsourcings im Gesundheitswesen	117
I. Konzept	117
1. Rechner beim Kunden	117
a. Anbindung der bildgebenden Verfahren an den e-pacs Department Server	118
b. Integration als Langzeitspeicher in ein bestehendes PACS-System	118
c. Ver- und Entschlüsselung der Daten	119
d. Lokale Speicherung der Daten	119
e. Fernwartung	119
2. Rechner im Archiv	119
a. Speicherung	120
b. Wiederaufruf	120
3. Datenübertragung	120

4. Verschlüsselung	121
a. Schlüsselmanagement	121
b. Komprimierung	122
c. Verschlüsselung und Abspeicherung	122
5. Datenarten	122
6. Gesicherte Rechnerräume	122
II. Analyse	123
1. Ärztliche Schweigepflicht	123
2. Datenschutzrecht	124
a. Verfügbarkeit	125
b. Integrität	126
c. Verbindlichkeit	126
d. Vertraulichkeit	126
e. Revisionsfähigkeit	127
f. Authentizität der Nutzer	128
III. Ergebnis	128
7. Teil: Rechtliche Anforderungen an die Vertragsgestaltung von Outsourcingprojekten	129
I. Rechtliche Einordnung der Verträge zur externen Archivierung von Patientendaten	129
1. Einordnung des Rechenzentrumsvertrages	129
2. Einordnung des Service-Rechenzentrumsvertrages	130
a. Mietvertrag	130
b. Dienstvertrag oder Werkvertrag	130
aa. Dienstleistung oder Werk geschuldet?	131
bb. Weisungsfreiheit und Eigenverantwortung	131
cc. Wartungsvertrag als Werkvertrag	132
dd. Ergebnis	132
ee. Judikatur	132
ff. Rechtsfolgen	132
II. Wichtige Vertragsbestandteile	133
1. Präambel und Begriffsbestimmungen	134
2. Vertragsgegenstand und Leistungspflichten	134
3. Übernahmebestimmungen	135
4. Personalübergang	135
5. Regelungen für Störfälle	136
6. Gewährleistungs- und Haftungsregelungen	136
7. Vertragsanpassungen, Lenkungsausschuss	137

8. Nutzungsrechte	137
9. Datenschutz und Datensicherheit	138
10. Vertragslaufzeit	139
11. Wechsel des IT-Anbieters	139
12. Kündigung und nachvertragliche Pflichten	139
13. Insolvenz	140
III. Ergebnis	141
8. Teil: Exkurs: Outsourcing ins Ausland	143
9. Teil: Schluss	145
Literaturverzeichnis	147