Rainer Braunschweig, Ivo Geis, Dieter Tolksdorf und Ilka Hansen

DOI: 10.1007/s00350-004-1198-2

# DACS[1] – Data Archiving and Communication Services

## Zentrale digitale Archivierung von Krankenhausdaten – ein ASP-Konzept

### Einleitung

Die wissenschaftlich-technische Entwicklung in der Medizin, die Bevölkerungsentwicklung, – insbesondere die Altersstruktur –, die Kostenexplosion von Einzelleistungen und die Finanzsituation der Kostenträger haben zu umfangreichen innovativen Finanzkonzepten geführt. Herausragendes Beispiel ist die Einführung der DRG's (diagnosis related groups). Es handelt sich um eine fallbezogene Krankenhausfinanzierung. Der Gesetzgeber und die Kostenträger erwarten bei unverändert gedeckeltem Budget Effektivitätssteigerungen bei der Patientenbetreuung.

Der in den 1990er Jahren gestiegene Leistungsdruck auf die Krankenhäuser wird durch diese Finanzierungsansätze verschärft. Wesentliches Überlebenskriterium der Leistungserbringer (Krankenhäuser) wird der Zeitbedarf zur Versorgung einzelner Krankheitsgruppen sein. Den Krankenhäusern stehen für die Lösung dieser Herausforderung zwei prinzipielle Instrumentarien zur Verfügung:

(1.) Maximale Effektivitätssteigerung der Arbeitszeitressourcen. Dies bedeutet geänderte Arbeitszeitsysteme und weitere Leistungsdrucksteigerung für die pflegerischen und ärztlichen Mitarbeiter.

(2.) Den Krankenhäusern und ihren Trägern stehen Investitionsmaßnahmen zur Verfügung, die vor allem die Prozessabläufe der Häuser optimieren müssen.

Diese Ausgangssituation hat in den letzten Jahren zu erfolgreichen Installationen von *einzelnen* IT-Systemen[2] geführt wie KIS[3], RIS[4], PACS[5].

Treibende logistische und kommerzielle Kraft bei der Installation entsprechender Systeme sind

(a) die Workflow-orientierten Prozessvorteile und
(b) die erheblichen Einsparpotentiale,

die der Liquidität der Krankenhäuser in ihre Verbrauchsbudgets rückgeführt werden können.

Trotz dieser Vorteile stehen auch kritische und offene Themenkomplexe in der Diskussion. Beispielgebend sind zu nennen:

(a) wiederkehrende Konzepterneuerungen der IT-Lösungen,
(b) der politische Auftrag zur integrierten Versorgung und
(c) datenschutzrechtliche Fragen

### 1. Application Service Provider

Unter dem Begriff ASP (Application Service Provider) haben sich IT-technische Leistungsanbieter am Markt profiliert, die den genannten Herausforderungen (z.B. Telemedizin, zentrale Archivierung, Datenbankmanagement etc.) Lösungen gegenüberstellen. In dem erreichten Entwicklungsstand digitaler Bildarchivierungs- und Kommunikationssysteme (PACS) gewinnen dabei „zentrale digitale Archivierungslösungen" für Krankenhausdaten, insbesondere für Daten der bildgebenden Diagnostik (großvolumigster Anteil im Krankenhaus) ein herausragendes Interesse.

#### *1.1. Problemstellung*

Die Gewerblichen Berufsgenossenschaften der Bundesrepublik Deutschland unterhalten neun Schwerpunktkrankenhäuser u. a. zur Versorgung ihrer Versicherten. Dabei versteht sich der gesetzliche Versorgungsauftrag neben der versicherungsrechtlichen Seite insbesondere in der Zurverfügungstellung hochqualifizierter medizinischer Versorgungseinrichtungen zur Diagnostik, Behandlung und Rehabilitation berufsbedingter Verletzungen und Krankheiten.

Nach Implementierung von krankenhauseigenen IT-Systemen (KIS, RIS, PACS) sind die zu archivierenden Datenmengen mit bis zu 3 Tbyte[6]/a/Krankenhaus erheblich. Daher sind zentrale Archivierungen als Geschäftsmodell interessant.

Es stehen folgende Fragen zur Beantwortung:

(1.) Ist eine zentrale digitale Archivierung von Bilddaten technisch möglich?

(2.) Wie erfolgt der Datenversand?

(3.) Wie erfolgt das „Retrieve" der Bilddaten und welcher Zeitbedarf ist erforderlich?

(4.) Ist eine zentrale digitale Archivierung durch einen nicht medizinischen Anbieter datenschutzrechtlich in Deutschland realisierbar?

(a) Wem gehören die Daten?
(b) Wer darf zugreifen?

#### *1.2. Material und Methode*

Im Auftrag des Geschäftsführers des Vereins für berufsgenossenschaftliche Heilbehandlung Halle e.V. haben die BG Kliniken Bergmannstrost Halle/Saale, die Firma Agfa Deutschland GmbH&Cie KG. und Dr. Ivo Geis (Rechtsanwalt in Hamburg) ein Projektteam zur Durchführung einer Pilotinstallation gegründet. Ziel des Pilotprojektes war die Klärung oben genannter Fragen und die Vorlage eines detaillierten Ergebnisberichtes zu technischen Details und zur datenschutzrechtlichen Durchführbarkeit. Diese Ergebnisse werden Grundlage der weiteren strategischen Entscheidungen bei der Nutzung IT-gestützter Systeme sein.

#### *1.3. Konzeptphase*

Die Autoren haben folgendes Anforderungsprofil an eine zentrale digitale Archivierung formuliert:

(1.) Es werden Bilddaten archiviert (DICOM-Daten).

(2.) Die zentrale Archivierung muss Bilddaten 30 Jahre lang vorhalten und diese jederzeit zur Verfügung stellen.

(3.) Die Archivierung hat kontinuierlich zu erfolgen.

(4.) Die Bilddaten sind während des Bildversandes, während der Archivierung und während des Rückversandes vor dem Zugriff Dritter zu schützen.

Dr. med. *Rainer Braunschweig*, Berufsgenossenschaftliche Kliniken Bergmannstrost,
Direktor der Klinik für bildgebende Diagnostik und Interventionsradiologie, Halle/Saale,
Rechtsanwalt *Dr. iur. Ivo Geis*, Glockengießerwall 26,
D-20095 Hamburg (Korrespondenzadresse),
*Dieter Tolksdorf* und *Ilka Hansen*, beide Agfa AG, Köln

1) Beim Deutschen Patent- und Markenamt als Warenzeichen angemeldet.
2) Informationstechnologie-Systeme.
3) Krankenhausinformationssystem (engl. HIS).
4) Radiologieinformationssystem.
5) Picture Archiving Communication System.
6) Terrabyte.

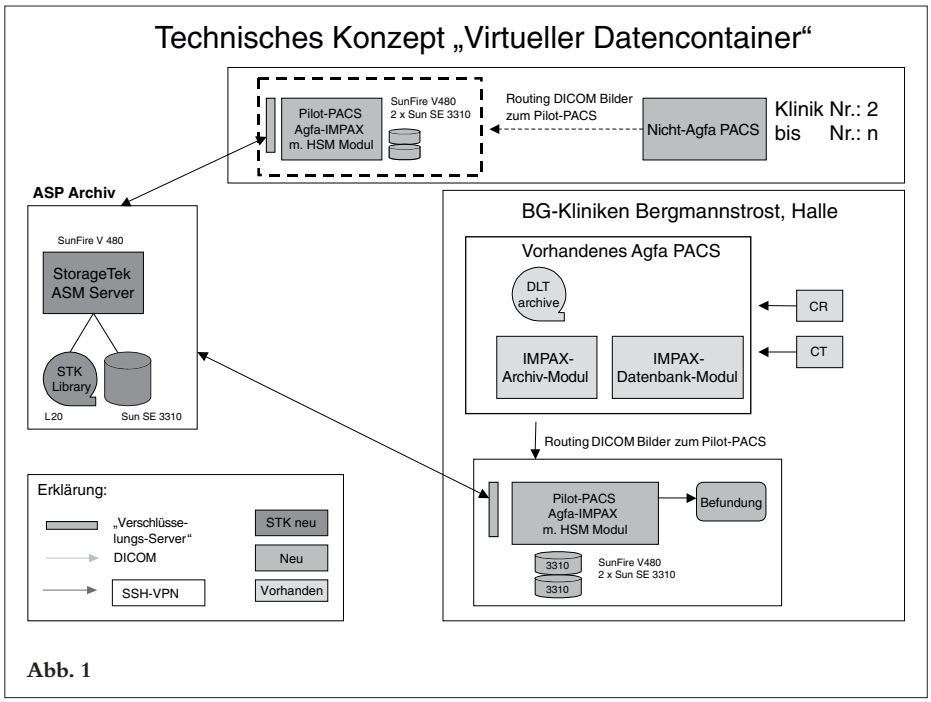


**Abb. 1**

(5.) Die Anforderungen des Datenschutzrechts müssen umgesetzt werden.

(6.) Das „Retrieve“ der Bilddaten muss arbeitstägig innerhalb von 12 Stunden und an Sonn- und Feiertagen innerhalb von 48 Stunden möglich sein.

## 2. Technisches Lösungskonzept für die Pilotphase

### *2.1. Angeschlossene Kliniken*

Für die Realisierung der Pilotstudie wurden zunächst in der BG Klinik Halle (Bergmannstrost) und später auch in der BG Klinik Bochum (Bergmannsheil) jeweils ein Pilot-PACS installiert. Es wurden aus Systemen in Halle und Bochum radiologische Untersuchungen im DICOM-Format in die jeweiligen Pilot-PACSysteme geroutet. Diese PAC-Systeme waren jeweils mit einem HSM-Modul ausgestattet, um die Kommunikation mit dem zentralen Archiv auf Basis von StorageTek ASM zu unterstützen (s. Abb. 1).

### *2.2. Aufbau ASP – Archiv*

Der Aufbau des zentralen Archivs erfolgte (pilotassoziiert) in der BG Klinik in Halle. Ein Unix-basiertes ASM[7]-System mit DLT-Jukebox kam für die Archivierung zum Einsatz (s. Abb. 1).

### *2.3. Netzwerk*

Um den datenschutzrechtlich sicheren Transport (Verschlüsselung/Digitale Signatur/Firewall) über die Kommunikationsnetze zu testen, wurden die Daten aus dem Pilot-PACS des Klinikums Bergmannstrost an einen externen Netzknoten geschickt, um dann durch die Firewall zurück in das zentrale Archiv ins Klinikum zu gelangen. Der Rücktransport der benötigten archivierten Daten erfolgte entsprechend. Der Datentransfer zwischen Client und Archiv wurde über die Einrichtung eines VPN[8] realisiert. Für das geforderte hohe Maß an Sicherheit wurde eine VPN-Verbindung eingerichtet, die über das Secure Shell (SSH) Protokoll gesichert wird. SSH ermöglicht sowohl die Verschlüsselung und kryptographische Identifizierung als auch die Integritätssicherung.

### *2.4. Virtueller Datencontainer*

Um den rechtlichen Datenschutzaspekten einer externen Archivierung gerecht zu werden, wurde eine technische Lösung mit dem Funktionsprinzip „virtueller Datencontainer“ der Firma Comcity aus Kiel eingesetzt. Mit dieser Lösung wird gewährleistet, dass die Daten beim Verlassen der (sicheren) Klinikumgebung verschlüsselt, über das Netzwerk transportiert und verschlüsselt auf dem Datenträger im Langzeitarchiv gespeichert werden (s. Abb. 2: Virtueller Datencontainer).

Vor Übertragung der Container wird die Identität des Zentralarchivs durch die absendende Stelle und im Gegenzug durch das Zentralarchiv die Identität der absendenden Stelle verifiziert und dadurch gegenseitig authentifiziert. Bei Anforderung eines Datencontainers durch eine berechtigte Stelle im Klinik-PACS wird der verschlüsselte Datensatz (in unserem Sinne: der geschlossene virtuelle Daten-Container) über das Netz an die anfordernde Stelle gesandt und erst beim Wiedereintreffen in der Klinikumgebung entschlüsselt. Die Realisierung erfolgt durch den Einsatz von Verschlüsselungsservern („encryption appliances“), die an strategischen Stellen im Netzwerk des Krankenhauses zum Einsatz kommen. Als Verschlüsselungsmethode wurde der AES Rijndael Algorithmus, ECB Code mit einem 256 bit Schlüssel verwendet.

## 3. Die rechtlichen Anforderungen

Elektronische Röntgenbilder, die von externen Dienstleistern elektronisch archiviert werden, müssen auf zwei Ebenen rechtssicher sein: Die Archivierung muss den Anforderungen des Datenschutzrechts entsprechen und für den Fall eines Rechtsstreits beweissicher sein.

### *3.1. Die Anforderungen des Datenschutzrechts*

Das Bundesdatenschutzgesetz (BDSG) schützt personenbezogene Daten, die in oder aus Dateien verarbeitet und ge-

7) ASM Asynchroner Storage Mode.
8) Virtuelles Privates Netzwerk.

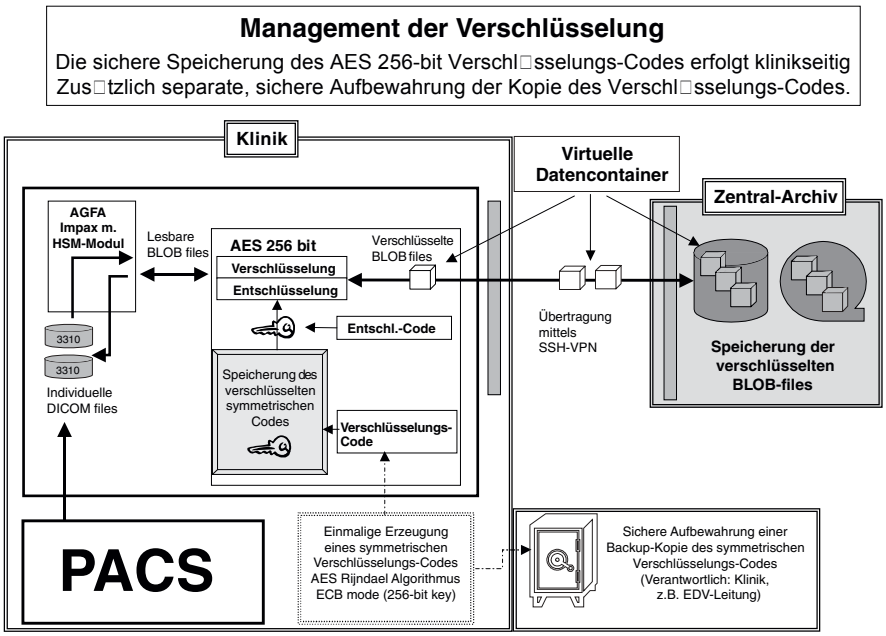


**Abb. 2.** Virtueller Datencontainer

nutzt werden. Datenschutz bedeutet, dass das Erheben, die Speicherung und die Verarbeitung personenbezogener Daten nur unter bestimmten Bedingungen und Grenzen zulässig ist. Für Gesundheitsdaten gelten zusätzliche Geheimhaltungspflichten, die um das ärztliche Standesrecht und das Strafrecht ergänzt werden.

### 3.1.1. Personenbezogene Daten, Gesundheitsdaten und Röntgenbilder

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 Abs. 1 BDSG. Die Einzelangaben über persönliche oder sachliche Verhältnisse einer Person umfassen alle Informationen über eine Person[9]. Damit ist für die Definition der personenbezogenen Daten ein weiter Begriff gewählt. Dieser umfasst Daten wie Name, Alter, charakterliche Eigenschaften und Gesundheit. Als Daten gelten auch die eine Person betreffenden Bildaufnahmen, also Informationen ohne sprachlich-symbolische Vermittlung[10]. Damit sind Röntgenbilder, die sich auf bestimmte Personen beziehen, personenbezogene Daten. Es ist unerheblich, auf welche Weise die Bezugsperson identifiziert werden kann[11]. Als Gesundheitsdaten sind Röntgenbilder gemäß § 3 Abs. 9 BDSG personenbezogene Daten besonderer Art. Hierfür gelten besonders strenge Schutzvorschriften, wenn sie erhoben, verarbeitet und genutzt werden.

### 3.1.2. Röntgenaufnahmen als Datenerhebung von Gesundheitsdaten

„Erheben" von Daten bedeutet das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG. Das Erheben der Daten muss gezielt erfolgen. Das Erheben umfasst das Erfragen besonderer Angaben und auch Bildaufnahmen bestimmbarer Personen[12]. Röntgenaufnahmen in der radiologischen Abteilung einer Klinik sind damit als Datenerhebung zu bewerten.

Die Erhebung besonderer Arten personenbezogener Daten wie von Gesundheitsdaten ist nur unter engen Voraussetzungen zulässig. Diese Voraussetzungen sind für Kliniken, die dem öffentlichen Bereich zuzurechnen sind, in § 13 Abs. 2 BDSG und für Kliniken, die dem nicht öffentlichen Bereich zuzurechnen sind, in § 28 Abs. 7 S. 1 BDSG gleich lautend geregelt. Die Datenerhebung von Gesundheitsdaten ist an den Grundsatz der Erforderlichkeit und an den Grundsatz der Geheimhaltung gebunden. Gesundheitsdaten dürfen zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung, der Behandlung oder für die Verwaltung von Gesundheitsdiensten erhoben werden, wenn dies erforderlich ist. Diese erforderliche Erhebung muss durch ärztliches Personal oder durch sonstige Personen erfolgen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

### 3.1.3. Klinische Auswertung der Röntgenbilder als Verarbeitung und Nutzung von Gesundheitsdaten

Werden elektronische Röntgenbilder klinisch ausgewertet, indem sie archiviert, an eine Stelle außerhalb der Klinik versendet und innerhalb der Klinik verwendet werden, so ist dies nach den Kategorien des Datenschutzrechts als Speicherung, Übermittlung und Nutzung zu bewerten.

Die Speicherung umfasst das Erfassen, Aufnehmen und Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung, § 3 Abs. 4 Nr. 1 BDSG. Datenträger ist ein weiter Begriff, der jedes Medium erfasst, auf dem personenbezogene Daten festgehalten werden können[13]. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten, also eine Stelle außerhalb der Klinik, § 3 Abs. 4 Nr. 3 BDSG. Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um deren Verarbeitung handelt (§ 3 Abs. 5 BDSG). Danach ist Nutzen die Auswertung von verarbeiteten Daten, die Verwendung des Informa-

9) *Dammann*, in: *Simitis* (Hrsg.), BDSG-Kommentar, 5. Aufl. 2003, § 3, Rdnr. 7.
10) *Dammann* (Fn. 9), § 3, Rdnr. 4.
11) *Dammann* (Fn. 9), § 3, Rdnr. 20.
12) *Dammann* (Fn. 9), § 3, Rdnr. 111.
13) *Dammann* (Fn. 9), § 3, Rdnr. 124.

tionsgehalts verarbeiteter Daten und die Weitergabe der Daten innerhalb der speichernden Stelle.

Die Aktivitäten einer radiologischen Abteilung erfüllen dieses datenschutzrechtliche Verhaltensmuster. Werden die radiologischen Aufnahmen in elektronischer Form archiviert, so werden sie gespeichert, werden sie an eine Stelle außerhalb der Klinik versendet, so werden sie übermittelt, und werden sie in elektronischer Form innerhalb der Klinik zu Diagnose- und Behandlungszwecken verwendet und verteilt, so werden sie genutzt.

Wie bei der Röntgenaufnahme als Datenerhebung, so bestehen auch für die weitere klinische Verwertung des Röntgenbildes die Geheimhaltungspflichten des ärztlichen Personals oder sonstiger Personen, die zu einer entsprechenden Geheimhaltung verpflichtet sind. Dies gilt gleichermaßen für den öffentlichen Bereich gemäß § 13 Abs. 5 Nr. 1 BDSG und für den nicht öffentlichen Bereich gemäß § 28 Abs. 7 S. 2 BDSG. Innerhalb der Klinik ist es durch organisatorische Maßnahmen möglich, die Geheimhaltungsvorschriften zu erfüllen. Problematisch ist die Übermittlung radiologischer Dokumente an externe Stellen. In diesen Fällen können Unberechtigte auf die Gesundheitsdaten zugreifen. Dadurch werden die datenschutzrechtlichen Geheimhaltungspflichten verletzt.

#### 3.1.4. Schutz von Gesundheitsdaten durch das ärztliche Standesrecht und das Strafrecht

Die Pflicht zur Geheimhaltung von Gesundheitsdaten hat neben dem datenschutzrechtlichen Aspekt auch einen standesrechtlichen und einen strafrechtlichen Aspekt. Das Arztgeheimnis ist Gegenstand der ärztlichen Berufsordnungen, die als autonomes Satzungsrecht der Landesärztekammern für die den Kammern angehörigen Ärzte verbindliches Recht setzen. Dieses Berufsgeheimnis bleibt durch das BDSG nach § 1 Abs. 3 S. 2 unberührt[14]. Wird die berufsrechtliche und datenschutzrechtliche Geheimhaltungspflicht verletzt, so hat diese unbefugte Offenbarung eines Geheimnisses die Strafbarkeit wegen Verletzung der ärztlichen Schweigepflicht gemäß § 203 StGB zur Folge[15]. Zum Offenbaren gehört nicht nur das gesprochene Wort, sondern auch schlüssiges Verhalten oder ein Unterlassen[16]. Somit ist Offenbaren auch gegeben, wenn eine Situation geschaffen wird, in der Unberechtigte auf die Gesundheitsdaten zugreifen können. Dies ist im Falle der externen Archivierung von Röntgenaufnahmen während des Transports der Daten durch das Netz und während der Archivierungsphase möglich.

#### 3.1.5. Ergebnis

Elektronische Röntgenbilder sind personenbezogene Gesundheitsdaten und unterliegen damit den Anforderungen des Bundesdatenschutzgesetzes. Diese besondere Art personenbezogener Daten darf nur zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erhoben, verarbeitet und genutzt werden. Die Erhebung, Verarbeitung und Nutzung dieser Daten muss durch ärztliches Personal oder durch sonstige Personen erfolgen, die einer entsprechenden Geheimhaltungspflicht unterliegen. In dieser umfassenden datenschutzrechtlichen Geheimhaltungspflicht für die Phasen der Erhebung, Verarbeitung und Nutzung liegt das Problem der externen elektronischen Archivierung, da die Gefahr besteht, dass die Daten den Kreis des berechtigten ärztlichen Personals überschreiten und von Unberechtigen zur Kenntnis genommen werden können. Dies bedeutet neben der Verletzung der datenschutzrechtlichen Geheimhaltungspflicht auch eine Verletzung der Geheimhaltungspflicht der ärztlichen Berufsordnung mit der Folge der Strafbarkeit nach § 203 StGB. Die externe Archivierung der Gesundheitsdaten benötigt damit ein rechtliches Lösungsmodell, das die Geheimhaltung sichert.

### *3.2. Rechtliche Lösungen für die externe elektronische Archivierung von Röntgenbildern*

Für die externe elektronische Archivierung von Röntgenbildern bestehen zwei rechtliche Alternativen: Die Einwilligung des Patienten und die Geheimhaltung durch Techniken des Zugriffsschutzes. Die Rechtsbeziehung zwischen Klinik und Archivdienstleister ist durch einen Vertrag zu gestalten, der an der Auftragsdatenverarbeitung des § 11 BDSG orientiert ist.

#### 3.2.1. Das Einwilligungskonzept

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen, § 4a Abs. 1 S. 1 BDSG. Deshalb ist der Betroffene nach § 4a Abs. 1 S. 2 BDSG auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen einer Einwilligungsverweigerung hinzuweisen. Für die Einwilligung ist grundsätzlich Schriftform erforderlich, § 4a Abs. 1 S. 3 BDSG. Wird die Einwilligung in Formularverträgen als Bestandteil der Allgemeinen Geschäftsbedingungen erteilt, so ist sie im äußeren Erscheinungsbild der Erklärung hervorzuheben, § 4a Abs. 1 S. 4 BDSG. Soweit besondere Arten personenbezogener Daten wie Gesundheitsdaten erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG. Dieses Einwilligungskonzept hat den Nachteil der Unberechenbarkeit: Die Funktionsfähigkeit des Archivierungssystems wird von der Bereitschaft der Patienten abhängig, die Einwilligung zu erteilen. Das Einwilligungskonzept ist auch aus einem anderen Aspekt problematisch. Es würde bedeuten, Patienten zu veranlassen, auf die Geheimhaltung ihrer Gesundheitsdaten zu verzichten. Dies berührt das durch Art. 1 GG geschützte Persönlichkeitsrecht, das nach § 1 Abs. 1 BDSG vor einer Beeinträchtigung geschützt werden soll. Die Einwilligung des Patienten in die externe elektronische Archivierung ist damit rechtlich unsicher. Die Geheimhaltung der Gesundheitsdaten ist damit unabdingbar für ihre externe Archivierung. Dies ist durch Techniken des Zugriffsschutzes möglich.

#### 3.2.2. Techniken des Zugriffsschutzes

Eine technische Lösung für den Zugriffsschutz ist die Verschlüsselung der Gesundheitsdaten während des Transports und der Archivierung. Damit sind die Gesundheitsdaten wie in einem „virtuellen Container" dem Zugriff Unberechtigter entzogen. Wird die Lösung des virtuellen Containers gewählt, so verwaltet das Personal des Archivierungszentrums nicht personenbezogene Daten, sondern „virtuelle Container", die die Daten nur für das berechtigte Klinikpersonal zugänglich enthalten. Eine Pflicht zur Anwendung dieser Technik besteht nicht. So können Daten in einer Standleitung ausgetauscht werden, die sie vor dem Zugriff Unberechtigter schützt. Während der Archivierung dürfen die Daten durch das verarbeitende Personal nicht auf bestimmte Patienten bezogen werden können. Auch in diesem Fall ist die Wahl der Technik frei. Als Alternative zur Verschlüsselung besteht die Möglichkeit der Anonymisierung und Pseudonymisierung von Daten, deren „Entschlüsselung" dem berechtigten ärztlichen Personal vorbehalten ist.

---

14) *Gola/Schomerus,* BDSG, 7. Aufl. 2002, § 1, Rdnr. 25; und *Simitis*, in: *ders.* (Hrsg.) (Fn. 9), § 1, Rdnr. 180.
15) S. hierzu *Simitis* (Fn. 14), § 1, Rdnr. 179.
16) *Jähnke* (1989), in: LK/StGB, 10. Aufl., § 203, Rdnr. 44.

3.2.3. Vertrag zwischen Klinik und Archivdienstleister

Für die Gestaltung des Vertrages zwischen der Klinik als Auftraggeber und dem Archivierungszentrum als Auftragnehmer ist der in § 11 BDSG vorgezeichnete Inhalt des Vertrages über die Auftragsdatenverarbeitung die gegebene Orientierung, selbst wenn nicht Daten im Auftrag verarbeitet werden, sondern „virtuelle Container", die Daten unzugänglich für den Auftragnehmer enthalten. Für diese Rechtsbeziehung sind die Elemente der Auftragsdatenverarbeitung charakteristisch: die Hilfsfunktion der Auftragsdatenverarbeitung, die Pflichten des Auftraggebers als des Verantwortlichen für die Datenverarbeitung, die Form der Auftragserteilung und die Weisungsbindung des Auftragsnehmers. Die Auftragsdatenverarbeitung nach Sozialgesetzbuch und bestimmten landesrechtlichen Vorschriften stellt besonders strenge Anforderungen.

Datenverarbeitung als Hilfsfunktion:

Für die Datenverarbeitung im Auftrag gemäß § 11 BDSG ist die wichtigste Voraussetzung, dass die Erhebung, Verarbeitung und Nutzung lediglich in ihrer Hilfsfunktion für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert wird. Werden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke teilweise abgegeben oder erbringt der externe Datenverarbeiter über die technische Verarbeitung hinaus materielle vertragliche Leistungen mit Hilfe der überlassenen Daten, dann ist er nicht mehr bloßer Auftragnehmer, sondern wird selbst zur verantwortlichen Stelle. Die Datenweitergabe im Rahmen einer solchen „Funktionsübertragung" ist konsequenterweise als Übermittlung zu klassifizieren[17].

Pflichten des Auftraggebers:

Der Auftraggeber ist nach § 11 Abs. 2 S. 1 und 4 BDSG zur sorgfältigen Auswahl des Auftragnehmers verpflichtet. Wichtigster Maßstab für die Auswahl des Auftragnehmers ist nach § 11 Abs. 2 S. 1 BDSG die „Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen". Entscheidendes Kriterium hierfür ist, ob bei der beauftragten Stelle ein angemessener Datensicherungsstandard gewährleistet ist, der den Anforderungen des § 9 BDSG und der Anlage zu dieser Vorschrift entspricht. Dies gilt insbesondere für die in Nr. 6 der Anlage genannte „Auftragskontrolle", die sicherstellen soll, dass der Auftragnehmer mit den ihm anvertrauten Daten nur entsprechend den Weisungen des Auftraggebers umgeht[18]. Die Auswahlentscheidung setzt nach § 11 Abs. 2 S. 4 BDSG voraus, dass der Auftraggeber sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Jedenfalls sollte der Auftraggeber das bei der beauftragten Stelle realisierte Datensicherungskonzept zur Kenntnis nehmen[19]. Unabdingbare Voraussetzung ist gemäß § 11 Abs. 4 BDSG, dass die Mitarbeiter des Auftragnehmers auf das Datengeheimnis nach § 5 BDSG verpflichtet werden.

Form der Auftragserteilung:

§ 11 Abs. 2 S. 2 BDSG verlangt, dass der Auftrag schriftlich zu erteilen ist. In dem schriftlichen Vertrag sind die „Datenerhebung, -verarbeitung oder -nutzung" festzulegen. Damit sind die Phasen der Datenverarbeitung angesprochen. Zu fixieren sind ferner die „technischen und organisatorischen Maßnahmen" der Datensicherung. Sie müssen den Zeitraum vom Eingang der Daten beim Auftragnehmer bis zur Ablieferung beim Auftraggeber umfassen[20]. Schließlich sind „etwaige Unterauftragsverhältnisse" festzulegen, die durch die Einschaltung von Subunternehmern entstehen. Die Vergabe von Unteraufträgen darf vom Auftraggeber nur gestattet werden, wenn der Auftragnehmer zusichert, dass die ihm obliegenden Pflichten auch vom Unterauftragnehmer eingehalten werden[21].

Weisungsbindung des Auftragnehmers:

Der Auftragnehmer darf nach § 11 Abs. 3 S. 1 BDSG die Daten nur „im Rahmen der Weisungen des Auftraggebers" erheben, verarbeiten und nutzen. Unter „Weisungen" sind alle vom Auftragnehmer vertraglich übernommenen Pflichten in Bezug auf Art und Gegenstand der Erhebung, Verarbeitung oder Nutzung sowie die technisch-organisatorische Datensicherung zu verstehen. Hinzu kommen die Einzelweisungen im laufenden Auftragsverhältnis. Verboten sind dem Auftragnehmer insbesondere die Weitergabe oder Übermittlung der Daten an Dritte, die Auskunftserteilung an den Betroffenen, die Verwendung für eigene Geschäftszwecke, die Nutzung für andere Auftraggeber sowie die Fortsetzung der Speicherung nach Auftragsabwicklung[22].

Auftragsdatenverarbeitung nach Sozialgesetzbuch und Landesdatenschutzgesetzen:

Die Auftragsdatenverarbeitung von Sozialdaten ist mit § 80 Abs. 5 SGB X bereichsspezifisch geregelt. Hiernach ist die Auftragsvergabe an nicht öffentliche Stellen nur zulässig, wenn Störungen im Betriebsablauf vermieden werden und erhebliche Kostenvorteile entstehen. Diese bereichsspezifische Vorschrift zur Auftragsdatenverarbeitung geht gemäß § 1 Abs. 3 S. 1 BDSG den Vorschriften des BDSG vor[23]. Eine entsprechende Vorschrift für die Auftragsverarbeitung besteht nach den Landeskrankenhausgesetzen einiger Bundesländer[24]. Diese Vorschriften, die die Auftragsverarbeitung unter den strengsten Anforderungen regeln, sind kein rechtliches Hindernis für die externe Archivierung von Röntgenbildern, wenn durch die Zugriffstechniken die Geheimhaltung der Daten gewahrt wird, indem der externe Archivdienst keine Kenntnis von den Daten nehmen kann.

3.2.4. Ergebnis

Die datenschutzrechtliche Lösung für die externe Archivierung von elektronischen Röntgenbildern ist nicht ein Einwilligungskonzept, sondern sind Techniken des Zugriffsschutzes, um die Gesundheitsdaten während des Transports durch das Netz und während der Archivierungsphase geheim zu halten und damit das durch das Grundgesetz und das Bundesdatenschutzgesetz gewährleistete Persönlichkeitsrecht zu schützen. Der Vertrag zwischen Klinik und Archivdienstleister wird nach dem Vorbild der Auftragsdatenverarbeitung gestaltet. Der entscheidende Bestandteil des Vertrages ist eine Vereinbarung über die Techniken des Zugriffsschutzes, um die Gesundheitsdaten geheim zu halten.

*3.3. Beweissicherheit*

In einem Arzthaftungsprozess ist die Klinik als Beweismittel auf elektronisch archivierte Röntgenbilder angewiesen. Deren Beweisqualität wird damit zu einer wesentlichen rechtlichen Anforderung. Beweissicherheit entsteht durch

17) *Walz*, in: *Simitis* (Hrsg.) (Fn. 9), § 11, Rdnr. 18.
18) *Walz* (Fn. 17), § 11, Rdnr. 42.
19) *Walz* (Fn. 17), § 11, Rdnr. 45.
20) *Walz* (Fn. 17), § 11, Rdnr. 50.
21) *Walz* (Fn. 17), § 11, Rdnr. 51.
22) *Walz* (Fn. 17), § 11, Rdnr. 57.
23) Zum Vorrang tatbestandskongruenter Vorschriften eines Bundesgesetzes s. *Gola/Schomerus* (Fn. 14), § 1, Rdnr. 24; und *Simitis* (Fn. 14), § 1, Rdnrn. 161–173.
24) So § 7 Abs. 2 Gesundheitsdatenschutzgesetz NRW und § 6 Abs. 2 KrankenhausdatenschutzVO Brandenburg.

die Techniken des Zugriffsschutzes und durch die Archivierung nach den Grundsätzen der Ordnungsmäßigkeit.

3.3.1. Beweissicherheit durch Zugriffssicherheit

Ein elektronisches Dokument ist nicht Urkunde i.S. von § 416 ZPO, da es in materialisierter Form von dem Aussteller nicht unterzeichnet ist[25]. Damit unterliegt das elektronische Dokument, dessen Beweis gemäß § 371 Abs. 1 S. 2 ZPO durch Vorlegung oder Übermittlung einer Datei angetreten wird, als Objekt des Augenscheins der freien Beweiswürdigung des Gerichts gemäß § 286 ZPO. Die freie Beweiswürdigung wird bestimmt durch Hinweise auf die Integrität des Dokumentes. Das entscheidende Argument für die Integrität wird durch die Techniken des Zugriffsschutzes geliefert. Hierdurch sind die Daten vor unberechtigten Zugriffen geschützt und damit fälschungssicher.

3.3.2. Beweissicherheit durch ordnungsmäßige Archivierung

Röntgenaufnahmen sind gemäß § 28 Abs. 4 RöV bis zu zehn Jahre nach der letzten Untersuchung aufzubewahren. Näheres zur Aufbewahrung auf elektronischen Speichermedien ist in der RöV nicht geregelt. Allgemeingültige Regeln für die ordnungsmäßige Archivierung elektronischer Dokumente sind die Vorschriften des Steuerrechts und des Handelsrechts zur Aufbewahrung von Steuer- und Handelsbelegen. Diese Vorschriften hat das Bundesfinanzministerium mit Schreiben vom 7. 11. 1995 „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme" (GoBS)[26] und mit Schreiben vom 16. 7. 2001 „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU) interpretiert. Mit der Aufbewahrung entsprechend diesen Grundsätzen soll die elektronische Dokumentation gegen Änderungen geschützt werden[27]. Deshalb gilt die entsprechende Aufbewahrung als Indiz für die Beweissicherheit[28]. In dieser Beweissicherheit für einen möglichen Arzthaftungsprozess liegt der Wert der elektronischen Archivierung von Röntgenbildern nach den Grundsätzen der Ordnungmäßigkeit. Für die ordnungsmäßige Archivierung von Röntgenbildern kommt es auf ordnungsmäßige Speichersysteme, ordnungsmäßige Wiedergabe und ordnungsmäßige Verfahrensdokumentation an.

Ordnungsmäßige Speichersysteme:

Ordnungsmäßig sind alle Speichermedien: die CD-Rom, die nicht wiederbeschreibbare Platte, die wiederbeschreibbare Platte und das Speicherband. Das Speichermedium ist damit offen für technische Entwicklungen[29]. Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das jeweilige Speichermedium gesondert ausgeprägt sein können. Problematisch ist die Langfristarchivierung: Dokumente, deren Inhalt der vertraglichen oder deliktsrechtlichen Verjährung unterliegt, müssen über einen Zeitraum von 30 Jahren archiviert werden. Während dieses Zeitraums muss der Zugriff auf das Dokument möglich sein. Eine Lösung für dieses Problem muss in einem Migrationskonzept gefunden werden, durch das die Dokumente in der jeweils aktuellen Archivierungstechnologie während des Archivierungszeitraums verfügbar sind.

Ordnungsmäßige Wiedergabe:

Die Wiedergabe von aufbewahrungspflichtigen Informationen ist gemäß § 257 Abs. 3 HGB und § 147 Abs. 2 AO ordnungsmäßig, wenn der Zugriff innerhalb einer angemessenen Frist möglich ist. Nach dem Steuerbereinigungsgesetz ist diese Anforderung als „unverzüglich" definiert worden. In der zivilrechtlichen Definition heißt dies: ohne schuldhaftes Zögern. Hierzu muss das Dokument mit einem unveränderten Index versehen sein. Die Frist für das Lesbarmachen wird analog zu § 238 Abs. 1 S. 2 HGB nach den Verhältnissen des Einzelfalles zu bestimmen sein[30].

Ordnungsmäßige Verfahrensdokumentation:

Die Anforderungen an die Verfahrensdokumentation sind in den vom Bundesfinanzministerium mit Schreiben vom 7. 11. 1995 veröffentlichten Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)[31] definiert worden. Nach Textziffer 6 müssen aus der Verfahrensdokumentation Inhalt, Aufbau und Ablauf des Verfahrens vollständig ersichtlich sein. In der formalen Gestaltung ist der Anwender frei. Der Umfang der erforderlichen Verfahrensdokumentation richtet sich nach der Komplexität der DV-Buchführung. Bei fremd erworbener Software hat der Anwender weitgehende Verpflichtungen: Der Anwender ist für die Vollständigkeit und den Informationsgehalt der Verfahrensdokumentation verantwortlich.

3.3.3. Ergebnis

Für die Beweisqualität elektronisch archivierter Dokumente wie elektronischer Röntgenbilder sprechen Techniken des Zugriffsschutzes und die Ordnungsmäßigkeit der Archivierung. Durch Zugriffsschutz und ordnungsmäßige Archivierung entsteht Fälschungssicherheit, die im Rahmen der freien Beweiswürdigung das entscheidende Argument für die Beweisqualität ist.

*3.4. Fazit*

Werden Röntgenbilder während des elektronischen Transports und während der elektronischen Archivierung vor dem Zugriff Unberechtigter geschützt und ist nur den berechtigten Ärzten und dem berechtigten ärztlichen Personal der Zugriff möglich, so ist die Archivierung bei einem externen Dienstleister rechtlich zulässig, denn die Daten bleiben geheim. Der Zugriffsschutz und die Archivierung nach den Grundsätzen der Ordnungsmäßigkeit bewirken die Fälschungssicherheit und damit die Beweissicherheit der extern archivierten Röntgenbilder.

## 4. DACS Data Archiving and Communication Services

Einige der hochmodern ausgestatteten Kliniken der Gewerblichen Berufsgenossenschaften in Deutschland haben mit der Installation von digitalen Akquisitions- und hausbezogenen Kommunikationssystemen eine Vorreiterrolle bei IT-basierten Konzepten eingenommen.

Unter dem Sammelbegriff DACS (Data Archiving and Communication Services) haben wir nunmehr einen zweiten Schritt digitaler Integration konzipiert. In der Pilotphase haben wir ein

(a) technisches,
(b) klinisch konzeptionelles und
(c) datenschutzrechtlich unbedenkliches

25) Allgemeine Meinung: *Geis* (2001), in: *Hoeren/Sieber* (Hrsg.), Handbuch Multimediarecht, Teil 13.2, Rdnrn. 5–8; *Oertel,* MMR 2001, 419; *Greger*, in: *Zöller*, ZPO, 21. Aufl. 1999, § 371, Rdnr. 1; Begründung der Bundesregierung, BT-Dr. 14/4987, S. 23, 25.
26) BStBl. I 1995, 738 ff.
27) *Kirnberger*, in: *Glanegger* u.a., HK/HGB, 6. Aufl. 2002, § 257, Rdnr. 3; *Ballwieser*, in: MüKo/HGB, Bd. 4, 2001, § 257, Rdnr. 16; *Walz*, in: Heymann, HGB, Bd. 3, 2. Aufl. 1999, § 257, Rdnr. 6.
28) *Wiedemann*, in: *Ebenroth/Boujong/Joost* (Hrsg.), HGB, 2001, § 257, Rdnr. 1.
29) *Ballwieser* (Fn. 27), § 257, Rdnr. 15; *Walz* (Fn. 27), § 257, Rdnr. 8; *Wiedemann* (Fn. 28), § 257, Rdnr. 24.
30) *Wiedemann* (Fn. 28), § 257, Rdnr. 25.
31) BStBl. I 1995, 738 ff.

Gesamtsystem entwickelt und an mehreren Kliniken erfolgreich getestet. Das Zertifikat und die Genehmigung des Bundesdatenschutzbeauftragten liegen vor.

Die Transferzeiten stören den klinischen Betrieb nicht. Wartungsarbeiten, Konzepterneuerungen und wiederkehrende Reinvestitionen sind für die Kliniken selbst entbehrlich. Das Archivierungsvolumen hat eine Größenordnung, die einen wirtschaftlichen Betrieb erlaubt und für die Einzelhäuser eine deutliche Kosteneinsparung pro gespeichertem Gbyte im Vergleich zur eigenen lokalen digitalen Archivierung darstellt. Es konnte mit Rechtsexperten und dem Bundesdatenschutzbeauftragten ein den aktuellen Anforderungen des Datenschutzes in Deutschland genügendes Schutzsystem entwickelt werden (virtueller Container). Die sonst im Einzelfall erforderliche Patienteneinwilligung zur Verarbeitung Patienten-assoziierter Daten entfällt. Damit wird der klinische Routinebetrieb vereinfacht und planbar. Das Selbstbestimmungsrecht und das Schutzbedürfnis der Patienten ist im Maße der bundesdeutschen Gesetzgebung respektiert

### 5. Zusammenfassung

1. Die gesundheitspolitischen Herausforderungen zur Sicherstellung einer hochqualitativen Patientenversorgung in Deutschland haben in innovativen Krankenhausgruppen zur Installation Workflow-unterstützender IT-Systeme geführt (KIS, RIS, PACS).

2. Der Druck zur integrativen Versorgung zwischen den Krankenhäusern und ambulanten Versorgungseinrichtungen hat den Datenkommunikationsbedarf gesteigert. Dieser ist mit analogen Mitteln nicht mehr anforderungskonform und zeitnah zu realisieren. Mit DACS steht im Sinne eines ASP-Konzeptes ein zentrales Archivierungskonzept für Krankenhausdaten zur Verfügung.

3. DACS ist durch den Bundesdatenschutzbeauftragten zertifiziert.

4. Ab einem Gesamtdatenvolumen von ca. 15 TByte pro Jahr sind zentrale Archivierungssysteme im Sinne von DACS wirtschaftlich zu betreiben.

5. Die Autoren empfehlen die flächenübergreifende Einführung entsprechender Systeme. Zu berücksichtigen sind
(a) einheitliche Standards (DICOM, HL7),
(b) zeitnahe und
(c) datenschutzrechtlich unbedenkliche Datenkommunikationstechniken.

---

Jan Tibor Lelley und Jan Vincent Sabin

# Entwicklungsklauseln in Chefarztverträgen – Reichweite des Direktionsrechts des Krankenhausträgers

**Zugleich Anmerkung zu BAG, Urt. v. 13. 3. 2003 – 6 AZR 557/01**

## I. Einleitung

Ein Urteil des BAG vom 13. 3. 2003[1] bietet Anlass, einen genaueren Blick auf die rechtlichen und unternehmerischen Konsequenzen von Entwicklungsklauseln in Chefarztverträgen zu werfen. Derartige Klauseln werden regelmäßig in den zwischen Krankenhausträger und leitendem Arzt (Chefarzt) geschlossenen Anstellungsverträgen vereinbart. Das Urteil ist die Fortführung einer Rechtsprechung[2], die die Zulässigkeit von weitreichenden Organisationsverfügungen des Krankenhausträgers gegenüber dem angestellten Chefarzt, die sich in der Praxis meist auf derartige Entwicklungsklauseln stützen, bestätigt.

Im Folgenden wird zunächst ein genereller Überblick über die arbeitsrechtliche Stellung eines leitenden Arztes (Chefarztes) in einem Krankenhaus gegeben, um dann darauf aufbauend die Tragweite von Entwicklungs- und Anpassungsklauseln in Chefarztverträgen, unter Berücksichtigung der Entscheidung des BAG vom 13. 3. 2003, zu untersuchen. Dabei wird insbesondere zu prüfen sein, wie weit eine Organisationsverfügung im Rahmen des Direktionsrechts des Arbeitgebers (Krankenhausträger) gegenüber dem Arbeitnehmer (Chefarzt) reichen kann, ohne dass es dazu einer Änderungskündigung bedarf.

## II. Rechtsstellung des Chefarztes im Krankenhaus

### *1. Leitender Angestellter nach § 5 Abs. 3 BetrVG und § 14 Abs. 2 KSchG sowie vergleichbare Stellung nach kirchlichem Dienstrecht*

Es ist mittlerweile einhellige Auffassung, dass Chefärzte im Verhältnis zum Krankenhausträger als Arbeitnehmer anzusehen sind. Die für die Arbeitnehmereigenschaft erforderliche persönliche Abhängigkeit vom Arbeitgeber ist zu bejahen, obwohl Chefärzte nach der hierarchischen Leitungsstruktur im Krankenhaus als auch im Hinblick auf die Freiheit des ärztlichen Berufs bei dessen Ausübung keinen Weisungen des Krankenhausträgers unterworfen sind[3]. Das BAG hat in einer Entscheidung dazu festgestellt, dass der Chefarzt, „wenn er auch grundsätzlich in der Ausübung seines ärztlichen Berufes eigenverantwortlich tätig ist, er im Übrigen im Wesentlichen weisungsgebunden und damit vom Krankenhausträger persönlich abhängig ist“[4].

Dagegen ist die Frage nach der arbeitsrechtlichen Qualifizierung von Chefärzten als leitende Angestellte i. S. von § 5 Abs. 3 BetrVG und § 14 Abs. 2 KSchG in Rechtsprechung und Schrifttum weithin umstritten[5].

---

Rechtsanwalt *Dr. iur. Jan Tibor Lelley* und
Rechtsreferendar *Jan Vincent Sabin*, LL.M.,
Kanzlei Buse Heberer Fromm, Huyssenallee 86-88, D-45128 Essen

1) BAG 13. 3. 2003, MedR 2004, 390 (in diesem Heft) = DB 2003, 1960 = AP BGB § 611 Arzt-Krankenhaus-Vertrag Nr. 47.
2) BAG 15. 12. 1976, AP BGB § 611 Arzt-Krankenhaus-Vertrag Nr. 3; BAG 9. 1. 1980, BAGE 32, 265; BAG 4. 5. 1983, BAGE 42, 336; BAG 28. 5. 1997, MedR 1997, 513 ff. = NZA 1997, 1160 ff.
3) *Richardi*, in: Münchener Hdb. d. ArbR, 2. Aufl. 2000, § 204, Rdnr. 3.
4) BAG 27. 7. 1961, AP BGB § 611 Ärzte, Gehaltsansprüche Nr. 24.
5) Vgl. zum Streitstand *Diringer*, NZA 2003, 890 ff. m.w.N.