DOI: 10.1007/s00350-013-3427-z

Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht

Benedikt Buchner

Der ärztliche Behandlungsalltag wird zunehmend komplexer, egal ob es um Dokumentation, Abrechnung oder IT geht. Ärztinnen und Ärzte sind daher mehr und mehr auf eine Einbindung externer Dienstleister angewiesen, um diesen Behandlungsalltag zu bewältigen. Problematisch ist eine solche Einbindung externer Dienstleister (Outsourcing) jedoch immer dann, wenn damit auch eine Offenbarung von Patientendaten gegenüber diesen Dienstleistern einhergeht. Der Patient muss sich darauf verlassen können, „dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt“[1]. Nur dann bleibt die Vertraulichkeit ärztlicher Behandlung gewahrt, die zentrales und unverzichtbares Element jeder Arzt/Patient-Beziehung ist.

Rechtlich wird die Vertraulichkeit der Arzt/Patient-Beziehung auf zweierlei Weise geschützt: zum einen durch das informationelle Selbstbestimmungsrecht des Patienten, wie es im BDSG und in bereichsspezifischen Datenschutzvorschriften seine einfachgesetzliche Ausgestaltung gefunden hat, und zum anderen durch die Schweigepflicht des Arztes, geregelt in den ärztlichen Berufsordnungen sowie strafrechtlich abgesichert in § 203 Abs. 1 Nr. 1 StGB. Sämtliche Formen eines Outsourcings müssen sich an diesen beiden Prinzipien messen lassen. Schwierigkeiten wirft dies vor allem deshalb auf, weil gerade beim Thema Outsourcing das Zusammenspiel zwischen informationeller Selbstbestimmung und ärztlicher Schweigepflicht noch in mancherlei Hinsicht ungeklärt ist und je nach Sichtweise die rechtlichen Hürden für eine Zulässigkeit des Outsourcings sehr hoch angesetzt sind[2].

I. Ausgangspunkt

Im Ausgangspunkt fußen informationelle Selbstbestimmung des Patienten und Schweigepflicht des Arztes auf demselben Regelungsprinzip: dem Verbotsprinzip mit Erlaubnisvorbehalt. Grundsätzlich ist eine Offenbarung von Patientendaten verboten, es sei denn, eine solche ist gesetzlich vorgesehen oder der Patient selbst hat darin eingewilligt. Letztere Einwilligung spielt sowohl im Datenschutzrecht als auch im Rahmen der ärztlichen Schweigepflicht eine zentrale Rolle, indem sie eine Datenverarbeitung gemäß § 4 Abs. 1 BDSG legitimiert bzw. zur Offenbarung von Patientendaten i. S. von § 203 StGB, § 9 MBO-Ä „befugt“. Auch für das Outsourcing gilt daher zunächst einmal, dass eine damit einhergehende Offenbarung von Patientendaten gegenüber externen Dienstleistern nur dann zulässig ist, wenn dies entweder gesetzlich erlaubt oder durch eine Einwilligung des Betroffenen legitimiert ist.

Prof. Dr. iur. Benedikt Buchner, LL.M. (UCLA),
Institut für Informations-, Gesundheits- und Medizinrecht,
Universität Bremen,
Postfach 33 04 40, 28334 Bremen, Deutschland

1. Outsourcing als Auftragsdatenverarbeitung

Eine gewisse datenschutzrechtliche Privilegierung erfährt das Outsourcing jedoch im Falle einer sog. Auftragsdatenverarbeitung gemäß § 11 BDSG[3]. Der Vorschrift des § 11 BDSG liegt die Idee einer Einheit von Auftraggeber und Auftragnehmer zugrunde. Beide werden vom Gesetz als eine rechtliche Einheit behandelt – mit der Konsequenz, dass der Auftragnehmer kein „Dritter“ im datenschutzrechtlichen Sinne ist. Damit ist dann auch eine Weitergabe personenbezogener Daten seitens des Auftraggebers an den Auftragnehmer datenschutzrechtlich irrelevant und es bedarf, anders als für eine Datenübermittlung i. S. des BDSG, keines datenschutzrechtlichen Erlaubnistatbestands für diese Datenweitergabe.

Abzugrenzen ist die Auftragsdatenverarbeitung von der sog. Funktionsübertragung. Letztere zeichnet sich dadurch aus, dass sich hier die beauftragte Stelle nicht auf eine bloße Hilfs- oder Unterstützungstätigkeit beim Prozess der Datenverarbeitung beschränkt, sondern dass diese Stelle bestimmte Aufgaben und Funktionen vollständig übernimmt und einen bestimmten Aufgabenbereich vollumfänglich erledigt. Von solch einer Funktionsübertragung ist etwa auszugehen, wenn eine externe Abrechnungsstelle nicht nur das Erstellen und Versenden von Rechnungen übernimmt, sondern darüber hinaus auch das Inkasso bei Zahlungsverzug. Gleiches gilt, wenn ein externes Callcenter sich nicht nur auf eine Kommunikationsvermittlung zwischen Arzt und Patient beschränkt, sondern den gesamten Patientenempfang (administrative Aufnahme und Arztzuweisung mit Zugriff auf die Patientendatei) abwickelt[4]. Regelmäßig zeichnet sich eine solche Funktionsübertragung auch dadurch aus, dass die beauftragte Stelle weitestgehend eigenverantwortlich und weisungsunabhängig tätig wird und der „Auftraggeber“ auf die einzelnen Phasen der Datenverarbeitung keinen Einfluss mehr ausübt. Handelt es sich um eine solche Funktionsübertragung, greift die Privilegierung der Auftragsdatenverarbeitung durch § 11 BDSG nicht ein, es handelt sich vielmehr um einen klassischen Übermittlungstatbestand, der entweder mittels Einwilligung oder auf der Grundlage eines gesetzlichen Erlaubnistatbestands legitimiert sein muss.

Beschränkt sich die externe Dienstleistung dagegen auf eine Auftragsdatenverarbeitung i. S. des § 11 BDSG, stellt sich für den Auftraggeber nicht das Problem, dass er für eine Weitergabe personenbezogener Daten an den Auftragnehmer einer Erlaubnis qua Gesetz oder Einwilligung bedarf. Ausreichend ist vielmehr, die Vorgaben, wie sie in

1) S. schon BVerfGE 32, 373, 380.
2) Der Beitrag konzentriert sich auf den Datenschutz in der Arztpraxis. Zu unterscheiden hiervon ist der Patientendatenschutz im Krankenhaus, für den insbesondere aufgrund der Regelungen im Landeskrankenhausrecht teils andere Maßstäbe gelten.
3) *Petri*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 11, Rdnr. 43.
4) Beispiele bei *Menzel*, in: *Buchner* (Hrsg.), Datenschutz im Gesundheitswesen, 2012, G/3, S. 23.

§ 11 BDSG detailliert normiert sind, zu erfüllen, also insbesondere in die schriftliche Auftragserteilung all die Mindestbestandteile aufzunehmen, wie sie in Nrn. 1–10 des § 11 Abs. 2 BDSG detailliert aufgeführt sind.

2. Problem ärztliche Schweigepflicht

Die (datenschutzrechtliche) Privilegierung der Auftragsdatenverarbeitung durch § 11 BDSG läuft allerdings leer, soweit es sich um eine Weitergabe von Daten handelt, die einem Berufsgeheimnis wie der ärztlichen Schweigepflicht unterfallen. Nach allgemeiner Meinung soll § 11 BDSG nicht in dem Sinne verstanden werden können, dass er auch eine „Befugnis" zur Offenbarung von Daten verleihe, die der ärztlichen Schweigepflicht unterfallen[5]. Damit bedarf es also, um nicht gegen die ärztliche Schweigepflicht zu verstoßen, einer anderweitigen Befugnis, um eine Preisgabe von Patientendaten legitimieren zu können.

An sich kommen als Legitimationsnormen zunächst einmal die Vorschriften des BDSG in Betracht. Allerdings stellt nicht nur § 1 Abs. 3 S. 2 BDSG, sondern auch § 28 Abs. 7 S. 2 BDSG klar, dass das BDSG insoweit hinter die Grundsätze der ärztlichen Schweigepflicht zurückzutreten hat, weshalb die Vorschriften des BDSG als möglicher gesetzlicher Erlaubnistatbestand ausscheiden. Bereichsspezifische Erlaubnistatbestände für eine Auslagerung bestimmter Dienstleistungen, wie sie sich für den Krankenhausbereich teils im Landeskrankenhausrecht finden lassen[6], existieren für den Bereich der Arztpraxen nicht. Im Ergebnis sind daher Ärzte auf die Einholung einer entsprechenden Einwilligung angewiesen.

In vielen Konstellationen wird sich dieser Weg jedoch als kaum praktikabel erweisen und/oder mit Rechtsunsicherheit behaftet sein. Das Einholen einer Einwilligung ist regelmäßig bereits mit einem erheblichen administrativen Aufwand verbunden. Unabhängig davon wird sich in manchen Konstellationen das Problem stellen, dass die Einholung einer Einwilligung überhaupt nicht möglich ist, weil es an einem unmittelbaren Kontakt zwischen Arzt und Patient fehlt[7]. Problematisch ist ebenso die Frage der Freiwilligkeit einer solchen Einwilligung, zumindest in den Konstellationen, in denen ein Patient offensichtlich auf eine ärztliche Behandlung angewiesen ist. Und schließlich stellt sich auch das Problem, dass es in manchen Konstellationen, etwa bei der Auslagerung von IT-Leistungen, praktisch unmöglich ist, für diejenigen Patienten, die eine solche Einwilligung nicht erteilen wollen, auf ein Outsourcing zu verzichten: die Wartung einer EDV-Anlage, die Datensicherung auf externen Speichern und ähnliche Dienstleistungen lassen sich sinnvoll nur dann auf externe Dienstleister übertragen, wenn davon alle Patientendaten erfasst werden.

II. „Datenschutzgesetzkonforme Auslegung" des § 203 StGB?

In Anbetracht des praktischen Bedürfnisses nach einem Outsourcing bestimmter Dienstleistungen im ärztlichen Behandlungsalltag verwundert es nicht, dass immer wieder der Versuch unternommen wird, diesem Bedürfnis rechtlich entgegenzukommen und Lösungsansätze zu entwickeln, die dem Arzt auch unter Geltung der ärztlichen Schweigepflicht in bestimmten Konstellationen eine Weitergabe von Patientendaten an externe Dienstleister erlauben. Verwundern kann dies auch deshalb nicht, weil hier offensichtlich ein Wertungswiderspruch zwischen Datenschutzrecht und ärztlicher Schweigepflicht besteht: Während das – an sich eher strenge – Datenschutzrecht bestimmte Formen einer Datenweitergabe offensichtlich als unproblematisch einordnet (jedenfalls dann, wenn die Sicherungsinstrumentarien, wie sie in § 11 BDSG normiert sind, beachtet werden), soll diese Wertung im Rahmen der ärztlichen Schweigepflicht keine Rolle spielen. Eben deshalb gehen aber auch die Versuche dahin, auf eine „datenschutzgesetzkonforme Auslegung"[8] des § 203 StGB hinzuwirken. Argumentativer Ansatz ist hierbei zum einen eine restriktive Auslegung des Begriffs des Offenbarens, zum anderen eine weite Auslegung des Gehilfenbegriffs i. S. des § 203 Abs. 3 S. 2 StGB.

1. Offenbaren

Ein restriktives Verständnis von „Offenbaren" wird insbesondere dann gefordert, wenn es sich bei Auftraggeber und Auftragnehmer um eine „informationelle Funktionseinheit" unter Steuerung des Auftraggebers handelt. Ein Offenbaren von Patientendaten gegenüber dem externen Dienstleister sei hier gerade nicht anzunehmen – vorausgesetzt, dieser externe Dienstleister ist aus Sicht des Patienten „in den organisatorischen und weisungsgebundenen internen Bereich der vertrauensbegründenden Sonderbeziehung einbezogen"[9]. Ist Letzteres der Fall, soll daher etwa die treuhänderische Abtretung ärztlicher Honorarforderungen und die damit verbundene Mitteilung von Patientendaten mangels „Offenbarens" nicht mehr unter § 203 StGB fallen[10].

Mit dem Abstellen auf eine „informationelle Funktionseinheit" wird an eine Argumentation angeknüpft, wie sie sich auch in der Rechtsprechung finden lässt. Auch die Rechtsprechung hat ein Offenbaren i. S. des § 203 StGB abgelehnt, wenn Patientendaten nicht „aus dem Kreis der Wissenden oder der zum Wissen Berufenen hinausgetragen werden", sondern „innerhalb bestimmter Funktionseinheiten (z. B. Behörde, Krankenhaus, Praxis)" verbleiben[11]. Ähnlich heißt es an anderer Stelle, dass die ärztliche Schweigepflicht auch im Falle der Abtretung ärztlicher Honorarforderungen noch gewahrt sei, wenn die Patientendaten „innerhalb des überschaubaren Bereichs des Krankenhauses" verbleiben[12]. Unproblematisch soll es daher sein, wenn einem Krankenhausträger die Einzugsermächtigung zur Geltendmachung von Chefarzthonoraren erteilt wird und es in diesem Zusammenhang auch zur Mitteilung der jeweiligen Patientendaten kommt[13].

Man mag in diesem Beispiel der Einzugsermächtigung zur Geltendmachung von Arzthonoraren durchaus argumentieren, dass es unter dem Aspekt der Vertraulichkeit keinen wesentlichen Unterschied mehr macht, ob nun der Chefarzt Patientendaten an die Verwaltungsabteilung des Krankenhauses weitergibt oder der Hausarzt an die privatärztliche Verrechnungsstelle – jedenfalls wenn Letztere unter Steuerung des verantwortlichen Arztes agiert. Gleichwohl ist kaum zu erwarten, dass die Rechtsprechung ein solch großzügiges Verständnis von einer „informationellen Funktionseinheit" unter Einbeziehung gerade auch externer Stellen übernehmen wird. Aus Sicht der Rechtsprechung ist vielmehr der entscheidende Unterschied, dass es sich im Falle externer Stellen um „außenstehende Dritte"

5) Vgl. *Petri*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 11, Rdnr. 44; *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 2012, Teil II, Kap. 2.7 (S. 259).
6) S. etwa § 48 Abs. 2 LKHG BB, Art. 27 Abs. 4 S. 5 u. 6 BayKrG, § 10 Abs. 3 BremKHDSG oder § 9 HmbKHG.
7) S. etwa im Falle von Laborärzten, Pathologen oder Konsiliarärzten (*Giesen*, NStZ 2012, 122, 123).
8) *Heghmanns/Niehaus*, NStZ 2008, 57, 60 f. m. w. N.
9) *Giesen*, NStZ 2012, 122, 128 (konkret zur Einschaltung privatärztlicher Verrechnungsstellen).
10) *Giesen*, NStZ 2012, 122, 128.
11) LG Bonn, NJW 1995, 2419, 2420 (zur Geltendmachung der Chefarzthonorare durch die Krankenhausträgerin).
12) LG Itzehoe, NJW 1993, 794.
13) LG Bonn und LG Itzehoe, jew. a. a. O.

handelt und damit eine Funktionseinheit eben nicht mehr angenommen werden kann[14].

Problematisch ist zudem, dass in den Fällen, in denen ein externer Dienstleister selbst nicht mehr einer Schweigepflicht unterfällt, eine mögliche weitere Datenpreisgabe durch diesen Dienstleister an andere Stellen im strafrechtsfreien Raum stattfinden und damit das Offenbarungsrisiko deutlich ansteigen würde. Im Falle des Outsourcings an Abrechnungsstellen stellt sich dieses Problem zwar insoweit nicht, als diese Stellen gemäß § 203 Abs. 1 Nr. 6 StGB ebenfalls einer Schweigepflicht unterfallen. Im Falle von IT- und anderen Dienstleistern aber fehlt es an einer vergleichbaren Regelung. Auch vor diesem Hintergrund scheidet daher im Ergebnis ein Anknüpfen an den Begriff des Offenbarens – jedenfalls als allgemein-gültiger Lösungsansatz – aus.

2. „Gehilfen-Lösung"

Die Gefahr einer Datenweitergabe im strafrechtsfreien Raum besteht von vornherein nicht, wenn man einen anderen argumentativen Ansatz wählt und von einem weiten Verständnis der Gehilfeneigenschaft i. S. des § 203 Abs. 3 S. 2 StGB ausgeht („Gehilfen-Lösung")[15]. Lassen sich auch externe Dienstleister als Gehilfen i. S. des § 203 Abs. 3 S. 2 StGB einordnen, werden diese in die schweigepflichtige Sphäre mit aufgenommen – mit der Konsequenz, dass eine Weitergabe von Patientendaten an diese Dienstleister straflos ist, sie ihrerseits aber bei einer unbefugten Weitergabe von Patientendaten wie Ärzte selbst nach § 203 StGB strafbar sind (befugte Mitwisser)[16].

Jedoch ist gerade streitig, ob auch externe Dienstleister Gehilfen i. S. des § 203 Abs. 3 S. 2 StGB sein können. Klassischerweise zählen zu diesen Gehilfen Personen, die gegenüber einem Schweigepflichtigen weisungsgebunden sowie in dessen Organisation und Pflichtenkreis eingebunden sind („Verantwortungseinheit")[17]. Nicht erfasst werden sollen demgegenüber selbständig tätige Personen, die lediglich bestimmte Aufträge für einen Schweigepflichtigen erledigen[18]. Wären auch solcherlei externe Dienstleister von der Strafandrohung des § 203 StGB erfasst, würde dies – so die Befürchtung – in Zeiten einer zunehmend arbeitsteilig organisierten Welt „ins Uferlose" führen[19].

Nach anderer Ansicht soll es sich demgegenüber jedoch auch im Falle externer Dienstleister um Gehilfen i. S. des § 203 Abs. 3 S. 2 StGB handeln können – vorausgesetzt der Dienstleister ist entsprechend organisatorisch eingebunden und der Auftraggeber (Schweigepflichtige) hat gegenüber diesem eine effektive Steuerungsmacht, weil ihm umfassende Kontroll- und Weisungsbefugnisse zustehen[20]. Empfohlen wird, diese Einbindung und Steuerungsmacht auch vertraglich umzusetzen, indem nach dem Vorbild des § 11 Abs. 2 BDSG detaillierte vertragliche Vereinbarungen getroffen werden und außerdem die Mitarbeiter des externen Dienstleisters nicht nur auf das Datengeheimnis nach § 5 BDSG, sondern auch auf eine Verschwiegenheit nach § 203 StGB verpflichtet werden[21]. Empfohlen wird außerdem die Vereinbarung entsprechender Vertragsstrafen, eine Beschränkung auf bestimmte Mitarbeiter, die beim externen Dienstleister die Tätigkeit übernehmen, und auch die Vereinbarung umfangreicher Gewährleistungspflichten[22].

Gerade mit Blick auf einen Wertungsgleichklang zwischen Datenschutzrecht und ärztlicher Schweigepflicht ist diese Gehilfenlösung zunächst einmal überzeugend. In Konstellationen, in denen das Datenschutzrecht eine rechtliche Einheit zwischen Auftraggeber und Auftragnehmer annimmt, scheint es nur konsequent, im Rahmen des § 203 StGB entsprechend von einer Gehilfeneigenschaft des Auftragnehmers auszugehen. Überdies ist ein solcher Ansatz durchaus auch im Sinne eines effektiven Datenschutzes, weil diese „Gehilfen" ebenfalls unter die Schweigepflicht des § 203 StGB fallen würden und damit eine neuerliche Weitergabe seitens dieser nicht im strafrechtsfreien Raum stattfinden würde.

Allerdings ist es gerade letzter Aspekt auch, der im Ergebnis dann doch entscheidend gegen die Gehilfen-Lösung spricht. Die Gehilfen-Lösung führt dazu, dass der Täterkreis des § 203 StGB ganz erheblich erweitert wird[23]. So überzeugend die Gründe hierfür sein mögen, ist es doch der Sache nach eine erweiternde Auslegung des § 203 Abs. 3 S. 2 StGB, die so weder vom Wortlaut noch von der ursprünglichen Regelungsintention des § 203 StGB gedeckt ist. Letztlich liegt damit ein Verstoß gegen das strafrechtliche Analogieverbot vor[24]. Gefragt ist daher der Gesetzgeber, der klarstellen muss, ob zum erweiterten Täterkreis des § 203 StGB nicht nur die klassischen Gehilfen zählen sollen, sondern auch externe Dienstleister, jedenfalls soweit diese organisatorisch eingebunden sind und einer effektiven Steuerungsmacht seitens des Auftraggebers unterliegen[25].

III. Punktuelle Lösungsansätze

Festzuhalten bleibt damit, dass es für das Outsourcing de lege lata nicht den einen umfassenden Lösungsansatz gibt. Die ärztliche Schweigepflicht setzt dem Outsourcing engere Grenzen als das Datenschutzrecht und es stellt sich die Frage, ob und wie diese Grenzen in den verschiedenen Fallkonstellationen überwunden werden können, um der teils mehr, teils weniger drängenden Notwendigkeit eines Outsourcings bestimmter Dienste Rechnung zu tragen. Anhand der Beispiele Cloud, Abrechnung und Callcenter soll dies im Folgenden erläutert werden.

1. Datensicherung in der Cloud

Der Trend zur papierlosen Praxis geht mit einem entsprechenden Bedürfnis nach externem IT-Sachverstand einher. EDV-Dokumentation setzt im Unterschied zur klassischen Patientenkartei spezifisches (IT-)Wissen voraus, das vom Arzt selbst – auch mit Blick auf die Schnelllebigkeit der informationstechnischen Rahmenbedingungen – nicht unbedingt erwartet werden kann. Gleiches gilt für die technisch-organisatorischen Maßnahmen, zu denen der Arzt unter dem Aspekt der Datensicherheit nach Maßgabe von § 9 BDSG verpflichtet ist. Unter anderem muss danach gewährleistet sein, dass „personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"[26]. Ebenso verpflichtet § 10 Abs. 5 MBO-Ä den Arzt zu besonderen

14) Vgl. LG Bonn, a. a. O.; aus der Literatur s. etwa *Cierniak,* in: MüKo/StGB, Bd. 4, 2. Aufl. 2012, § 203, Rdnr. 51 (keine Funktionseinheit bei externen Stellen).
15) Vgl. ausführlich dazu *Hartung*, VersR 2012, 400, 408 ff.
16) *Heghmanns/Niehaus*, NStZ 2008, 57, 58.
17) *Knauer/Brose*, in: *Spickhoff* (Hrsg.), Medizinrecht, 2011, §§ 203 ff. StGB, Rdnr. 23.
18) Vgl. *Biewald*, DuD 2011, 867, 867; *Cierniak,* in: MüKo/StGB, Bd. 4, 2. Aufl. 2012, § 203, Rdnr. 123.
19) *Schünemann,* in: LK/StGB, Bd. 6, 12. Aufl. 2009, § 203, Rdnr. 79.
20) *Heghmanns/Niehaus*, NStZ 2008, 57, 61 f.
21) *Hartung*, VersR 2012, 400, 409 f. Gegen eine Verpflichtung auf Verschwiegenheit nach § 203 StGB s. jedoch *Biewald*, DuD 2011, 867, 867: „Strafbarkeiten können nicht vereinbart werden".
22) *Hartung*, VersR 2012, 400, 409 f.
23) S. schon oben, Fn. 19.
24) Vgl. auch *Jandt/Roßnagel*, NZS 2011, 641, 645.
25) S. zu dieser Forderung bereits das Gutachten der Großen Strafrechtskommission des Deutschen Richterbundes v. 2007 (Kurzfassung bei *Kintzi*, DRiZ 2007, 244, 249).
26) Sog. Verfügbarkeitskontrolle; Anlage zu § 9 S. 1 BDSG, Ziff. 7.

Sicherungs- und Schutzmaßnahmen, um u. a. die Vernichtung von Aufzeichnungen auf elektronischen Datenträgern zu verhindern.

Umgesetzt werden kann diese Verpflichtung zur Datensicherung auf verschiedene Art und Weise, etwa durch eine Datensicherung auf einer zweiten Festplatte, auf DVDs etc. In Betracht kommt daneben auch die Nutzung von Servern in Form sog. Clouds, die von externen Dienstleistern betrieben werden. Im Vergleich zu traditionellen Speicherungsmedien bieten solcherlei Cloud-Dienste unter dem Aspekt der Datensicherheit manche Vorteile (Stichwort verlorener USB-Stick, entwendete Festplatte). Datenschutzrechtlich ist die Einbindung eines solchen externen Cloud-Dienstes als Auftragsdatenverarbeitung grundsätzlich möglich – vorausgesetzt es handelt es sich hierbei nicht um eine Funktionsübertragung[27], die Vorgaben des § 11 BDSG werden gewahrt und die Server stehen nicht im außereuropäischen Ausland[28]. Unter dem Aspekt der ärztlichen Schweigepflicht ist hingegen – da die Privilegierung als Auftragsdatenverarbeitung insoweit nicht gilt – entweder eine Einwilligung seitens der Betroffenen (Patienten) notwendig oder aber es muss sichergestellt sein, dass die auf der Cloud gesicherten Daten für den Betreiber der Cloud nicht personenbeziehbar sind, sei es weil dort nur pseudonymisierte Daten gespeichert werden, sei es weil die Daten entsprechend verschlüsselt sind[29].

a) Einwilligung

Der Erlaubnistatbestand der Einwilligung ist unter mehrerlei Gesichtspunkten problematisch, zuallererst schon mit Blick auf die praktischen Schwierigkeiten, von allen Patienten eine Einwilligung einzuholen. Problematisch ist die Einwilligungslösung vor allem aber auch deshalb, weil die externe Datensicherung in einer Cloud überhaupt nur dann praktikabel ist, wenn auch die Daten aller Patienten dort gespeichert werden können. Der Arzt müsste also darauf hinwirken, dass sich alle Patienten mit einer solchen externen Datenspeicherung einverstanden erklären – notfalls indem er die Einwilligung zur Vorbedingung für ein Behandlungsverhältnis macht („take it or leave it"). Damit stellt sich aber ein klassisches Freiwilligkeitsproblem und je nachdem, wie streng man das Gebot der Freiwilligkeit einer Einwilligung versteht, käme man hier möglicherweise zu einer Unwirksamkeit der erteilten Einwilligung – mit der Konsequenz, dass der Arzt unbefugt i. S. des § 203 StGB Patientendaten preisgegeben hat.

b) Technische Lösungen

Vorzugswürdig ist es daher, sich statt auf eine Einwilligung auf technische Lösungen zu stützen, die eine externe Datensicherung ermöglichen. In Betracht kommen hierfür etwa die Pseudonymisierung oder Verschlüsselung von Daten, so dass es von vornherein gar nicht zu einer Preisgabe von personenbezogenen Daten kommt. In Betracht kommen daneben aber auch technische Zugriffssperren, etwa Authentifizierungsmittel wie Passwörter oder Chipkarten, die gewährleisten, dass trotz Datenspeicherung auf einem externen Server dessen Betreiber selbst keinen Zugriff auf die gespeicherten Daten hat und es damit nicht zu einer Preisgabe von Patientendaten kommt[30].

c) Organisatorische Sperren

Fraglich ist, ob statt technischer Zugriffssperren auch bloße organisatorische Sperren ausreichen, um trotz Speicherung auf externen Servern eine „Offenbarung" von Daten ausschließen zu können. Solche organisatorischen Sperren könnten etwa so aussehen, dass Datenzugriffe seitens des Serverbetreibers ausdrücklich untersagt sind, dass sämtliche Zugriffe auf den Datenbestand kontrolliert und protokolliert sowie Verstöße gegen das Zugriffsverbot geahndet werden[31]. Dafür, dass auch derlei organisatorische Sperren reichen, spricht ein Vergleich mit der Übergabe von Patientendateien im Zuge einer Praxisübernahme. Für eine Wahrung der ärztlichen Schweigepflicht reicht es hier aus, wenn sich der Praxiserwerber – möglichst unter Vereinbarung einer Vertragsstrafe – dazu verpflichtet, die ihm übergebenen Patientendaten unter Verschluss zu halten (in einem Schrank, einem passwortgeschützten Praxisrechner o. Ä.) und nur dann darauf Zugriff zu nehmen, wenn sich ein Patient damit einverstanden zeigt[32]. Die bloße Möglichkeit des Zugriffs auf Patientendaten, wie sie in dieser Konstellation für den Erwerber eröffnet ist, begründet also offensichtlich noch keine „Offenbarung" i. S. des § 203 StGB. Entscheidend ist vielmehr, dass dem Praxiserwerber ein solcher Zugriff untersagt ist und dies auf mögliche Verstöße hin kontrolliert wird[33] (sowie ggf. auch sanktioniert wird). Auch insoweit handelt es sich also um eine bloße organisatorische Sperre, die für die Wahrung der ärztlichen Schweigepflicht ausreicht. Dies muss dann aber ebenso auch für andere Konstellationen gelten wie etwa die hier diskutierte Datensicherung auf Servern externer Anbieter.

2. Abrechnung über externe Stellen

Anders als im Fall der Datensicherung ist es bei einer Abrechnung über externe Stellen nicht möglich, mittels technischer oder organisatorischer Sperren eine „Offenbarung" von Patientendaten auszuschließen, da es für eine Abrechnung anders als für eine bloße Datensicherung gerade auf die Kenntnis der überlassenen Daten ankommt. Daher bedarf es einer anderen Legitimationsbasis.

a) Konkludente Einwilligung?

Als eine solche Legitimationsbasis kommt zunächst einmal die Einwilligung des Betroffenen selbst in Betracht, auf die in der Praxis auch regelmäßig zurückgegriffen wird. Fraglich ist, welche Form diese Einwilligung haben muss, insbesondere ob diese auch konkludent erteilt werden kann. Reicht es für die Annahme einer wirksamen Einwilligung in die Datenweitergabe an externe Abrechnungsstellen aus, dass sich der Patient in Kenntnis dieser Weitergabepraxis widerspruchslos in ärztliche Behandlung begibt?

In Betracht kommt dies von vornherein nur dann, wenn für die Erteilung einer Einwilligung nicht auch die Formvorgaben des BDSG zu berücksichtigen sind. Gemäß § 4a Abs. 1 S. 3 BDSG bedarf eine datenschutzrechtliche Einwilligung grundsätzlich der Schriftform, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist". Des Weiteren gilt für Gesundheitsdaten als „besondere Art personenbezogener Daten" i. S. des § 3 Abs. 9 BDSG die Vorgabe des § 4a Abs. 3 BDSG, wonach sich eine Einwilligung des Betroffenen gerade auch ausdrücklich auf diese Gesundheitsdaten beziehen muss. Nach den Vorgaben des BDSG kommt daher eine konkludente Einwilligung

27) Zur Abgrenzung s. oben, sub I. 1.
28) Vgl. *Petri*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 11, Rdnr. 30.
29) *Hartung*, VersR 2012, 400, 405 f.; s. schon OLG Düsseldorf, CR 1997, 536, 537, zur Zulässigkeit einer Archivierung von Patientendaten durch externe Dienstleister: entweder (ausdrückliche) Einwilligung der Patienten oder Archivierung mittels verschlossen zu haltender, anonymisierter Behältnisse, die äußerlich den Patientennamen nicht erkennen lassen.
30) *Hartung*, VersR 2012, 400, 405 f.
31) *Hartung*, VersR 2012, 400, 406 f.
32) *Menzel*, in: *Buchner* (Hrsg.), Datenschutz im Gesundheitswesen, 2012, G/7, S. 1 f.; *Schlund*, in: *Laufs/Kern* (Hrsg.), Handbuch des Arztrechts, 4. Aufl. 2010, § 19, Rdnr. 6.
33) Etwa durch einen Praxismitarbeiter in Vertretung des schweigepflichtigen Praxisveräußerers oder mittels Zugriffsprotokollierung im Falle der Übergabe eines Praxisrechners; vgl. *Menzel*, in: *Buchner* (Hrsg.), Datenschutz im Gesundheitswesen, 2012, G/7, S. 1 f.

im Fall der Verarbeitung von Gesundheitsdaten nicht in Betracht[34].

Ungeklärt ist allerdings, ob die Vorgaben des BDSG wiederum auch im Rahmen ärztlicher Schweigepflicht gelten und daher insoweit eine konkludente Einwilligung nicht in Betracht kommt. Die Rechtsprechung hat diese Frage bislang nicht abschließend entschieden. Der BGH hat sich mit der Zulässigkeit einer Einschaltung externer Abrechnungsstellen zwar schon vor über 20 Jahren befasst und damals die mit der Forderungsabtretung einhergehende Weitergabe von Patientendaten als Verletzung der ärztlichen Schweigepflicht eingeordnet, weil der Patient in diese Weitergabe nicht eingewilligt hatte[35]. Letztere Einwilligung wurde im konkreten Fall aber weder ausdrücklich noch konkludent erteilt, weshalb der Gerichtshof auch nicht entscheiden musste, ob eine konkludente Einwilligung als Legitimation für eine Offenbarung von Patientendaten überhaupt ausreichen würde oder für eine wirksame Einwilligung zusätzlich auch die Formvorgaben des BDSG zu berücksichtigen wären[36].

Selbst wenn man von der Zulässigkeit einer konkludent erteilten Einwilligung ausgehen wollte, ist diese allerdings unter dem Aspekt der Rechtssicherheit keine sonderlich verlässliche Legitimationsgrundlage. Nicht vertretbar wäre es, pauschal in jeder widerspruchslosen Inanspruchnahme ärztlicher Behandlung auch ein konkludentes Einverständnis mit einer Datenpreisgabe an externe Stellen zu sehen. Maßgeblich sind vielmehr die konkreten Umstände des Einzelfalls, wobei Zweifel zulasten des Arztes gehen. Auch der BGH lässt gewisse Vorbehalte gegenüber einer lediglich konkludent erteilten Einwilligung erkennen, wenn er darauf verweist, dass es mit Blick auf die ärztliche Schweigepflicht grundsätzlich am Arzt sei, die Einwilligung des Patienten „in eindeutiger und unmissverständlicher Weise" einzuholen. Umgekehrt sei es gerade nicht Sache des Patienten, einer Weitergabe seiner Daten zu widersprechen, um den Eindruck einer stillschweigenden Einwilligung zu vermeiden[37].

b) Gehilfen-Lösung

Von vornherein entbehrlich ist der Rückgriff auf die Einwilligung als Erlaubnistatbestand, wenn für Verrechnungsstellen ein Ausweichen auf die oben bereits angesprochene Gehilfen-Lösung in Betracht kommt. Oben wurde diese Lösung in erster Linie wegen Bedenken hinsichtlich einer unzulässigen Ausdehnung des Täterkreises einer Schweigepflichtverletzung abgelehnt. Dieses Problem stellt sich jedoch im Falle von externen Verrechnungsstellen nicht: Soweit diese unter § 203 Abs. 1 Nr. 6 StGB fallen, sind sie ohnehin vom Täterkreis des § 203 StGB erfasst. Ein Verstoß gegen das Analogieverbot wäre damit nicht zu befürchten, wenn externe Verrechnungsstellen auch als Gehilfen i. S. von § 203 Abs. 3 S. 2 StGB eingeordnet werden.

Allerdings kann eine solche Einordnung nicht pauschal für alle Formen einer Einschaltung externer Abrechnungsstellen in Betracht kommen, sondern lediglich dann, wenn es aus Patientenperspektive für die Vertraulichkeit der Arzt/Patient-Beziehung keinen wesentlichen Unterschied macht, ob die Patientendaten intern für Abrechnungszwecke verarbeitet werden oder eine externe Stelle damit betraut ist. Von vornherein kommt daher eine Gehilfeneigenschaft bei externen Abrechnungsstellen nicht mehr in Betracht, wenn diese auch mit dem Einzug ärztlicher Honorarforderungen befasst sind, egal ob im Wege der Einzugsermächtigung, der Inkassozession oder des Factoring. Beschränkt sich also die externe Dienstleistung nicht auf das Erstellen und Versenden der Rechnungen, sondern umfasst sie auch irgendeine Form des Inkasso- oder Forderungsmanagements, so ist ausgeschlossen, dass der externe Dienstleister noch ein „Gehilfe" i. S. des § 203 Abs. 3 S. 2 StGB ist. Mit einer solchen Differenzierung ist zugleich auch ein Wertungsgleichklang mit dem Datenschutzrecht hergestellt: Auch eine Auftragsdatenverarbeitung i. S. des § 11 BDSG ist nur dann anzunehmen, wenn sich die Dienstleistung einer Entgeltabrechnung auf bloße technische Hilfsfunktionen beschränkt[38]. Übernimmt der Dienstleister hingegen auch das Inkasso- oder Forderungsmanagement, handelt es sich nicht mehr um eine Auftragsdatenverarbeitung, sondern um eine Funktionsübertragung – mit der Konsequenz, dass solch ein Dienstleister echter „Dritter" i. S. des BDSG ist und es für eine Datenübermittlung an ihn einer Einwilligung oder eines gesetzlichen Erlaubnistatbestands bedarf.

Im Ergebnis kann also im Falle der Einschaltung externer Verrechnungsstellen auf die Gehilfen-Lösung zurückgegriffen werden, wenn folgende Voraussetzungen erfüllt sind: Die Dienstleistung muss sich auf bloße technische Hilfsfunktionen beschränken (Erstellen und Versenden der Abrechnungen), der Dienstleister muss organisatorisch eingebunden sein und der Schweigepflichtige (Arzt) muss umfangreiche Kontroll- und Weisungsbefugnisse gegenüber diesem haben („effektive Steuerungsmacht")[39]. In allen anderen Fällen bleibt es dabei, dass es für die Legitimation einer Einschaltung externer Abrechnungsstellen einer ausdrücklichen Einwilligung der betroffenen Patienten bedarf.

3. Patientenkommunikation mittels Callcenter

Schalten Arztpraxen zur Entlastung ihres Empfangsbereichs externe Callcenter für die Terminvereinbarung und Patientenkommunikation ein, stellt sich auch hier die Frage, ob und inwieweit dies mit Datenschutz und/oder ärztlicher Schweigepflicht vereinbar ist. Datenschutzrechtlich kann eine solche Einschaltung in Form einer Auftragsdatenverarbeitung nach § 11 BDSG zulässig sein – vorausgesetzt, das Callcenter beschränkt sich auf eine bloße Vermittlung der Kommunikation zwischen Arzt und Patient und erbringt im Einzelnen vorgegebene Serviceleistungen, ohne dabei einen eigenen Entscheidungsspielraum zu haben[40].

Problematisch ist aber wiederum die Wahrung der ärztlichen Schweigepflicht. Bereits der Umstand, dass jemand einen Arzttermin vereinbart, fällt unter die ärztliche Schweigepflicht; ob der Patient dem Callcenter zusätzlich auch irgendwelche Beschwerden oder Krankheitsbilder mitteilt, ist unerheblich. Auch eine „Offenbarung" der Patientendaten ist zu bejahen. Hierfür muss der Arzt nicht

34) Vgl. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 4a, Rdnr. 34.
35) BGH, NJW 1991, 2955.
36) Auch die weitere Rechtsprechung hat es bis heute in den meisten Fällen dabei bewenden lassen, die Frage offenzulassen, weil sie im konkreten Fall nicht entscheidungsrelevant ist. Mitunter wird die Frage explizit offengelassen – so etwa OLG Celle, BeckRS 2008, 20872: „Ob die Einwilligung eines Patienten zur Abtretung einer Forderung des behandelnden Arztes der Form des § 4a BDSG bedarf, hat der Bundesgerichtshof bislang ausdrücklich offen gelassen … Diese Rechtsfrage kann hier jedoch offen bleiben. Die Beklagte hat der Abtretung nämlich schriftlich zugestimmt". In anderen Fällen beschränken sich die Gerichte darauf, ohne weitere Erläuterungen festzuhalten, dass eine Einwilligung ohnehin schriftlich erteilt ist (OLG Karlsruhe, NJW 1998, 831, 832) bzw. noch nicht einmal konkludent erfolgt ist (OLG Düsseldorf, NJW 1994, 2421, 2422; OLG Köln, NJW 1991, 753, 754).
37) BGH, NJW 1991, 2955, 2957; ebenso auch BGH, NJW 1992, 2348, 2349; in letzterer Entscheidung schließt der BGH die Möglichkeit einer stillschweigenden Einwilligung zwar nicht aus, stellt aber hohe Anforderungen für die Annahme einer solchen.
38) Vgl. *Petri*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 11, Rdnr. 22.
39) Dazu schon oben bei Fn. 20.
40) Vgl. *Petri*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 11, Rdnr. 29.

von sich aus aktiv Patientendaten mitteilen, ausreichend ist vielmehr, dass er durch die Einschaltung eines Callcenters diesem die Möglichkeit verschafft, von Patientendaten Kenntnis zu erlangen. Schließlich kommt auch die „Gehilfen-Lösung" hier nicht in Betracht. Unabhängig davon, ob im konkreten Fall möglicherweise die Voraussetzungen einer organisatorischen Einbindung und effektiven Steuerungsmacht erfüllt wären, würde eine Einbeziehung externer Callcenter in den Täterkreis des § 203 StGB gegen das strafrechtliche Analogieverbot verstoßen[41]. Letztlich bleibt damit nur die Alternative, auf der Grundlage einer Einwilligung der Patienten die Einschaltung externer Callcenter zu legitimieren.

a) Formvorgaben des BDSG?

Praktikabel ist der Weg über die Einwilligung allerdings nur dann, wenn die Erteilung einer solchen Einwilligung nicht auch an die Formvorgaben des BDSG gebunden ist. Eben dies ist bis heute nicht abschließend geklärt[42].

Sicherlich gibt es Konstellationen, in denen die Formvorgaben des BDSG unstreitig nicht Geltung beanspruchen können. So würde es einen nicht nachvollziehbaren Formalismus bedeuten, müsste eine Einwilligung in die Datenweitergabe stets auch dann ausdrücklich oder schriftlich nach den Vorgaben des BDSG erfolgen, wenn diese Datenweitergabe für einen erfolgreichen Behandlungsablauf offensichtlich erforderlich ist, etwa die Datenweitergabe an den nachbehandelnden Arzt bei Einweisung ins Krankenhaus zur Weiterbehandlung oder die Datenweitergabe durch den Hausarzt bei Überweisung an den Facharzt[43].

Hiervon zu unterscheiden sind jedoch Konstellationen, in denen eine Datenweitergabe zwar mit einem ärztlichen Behandlungsverhältnis im Zusammenhang steht, aber für dessen Durchführung nicht erforderlich, sondern allenfalls hilfreich ist. In solchen Konstellationen sind über die Vorgaben der ärztlichen Schweigepflicht hinaus auch diejenigen des BDSG zu beachten, wenn Letztere strengere Datenschutzanforderungen aufstellen. In solchen Konstellationen reicht daher die konkludente Erteilung einer Einwilligung nicht mehr aus, zu fordern ist vielmehr die ausdrückliche und schriftliche Erteilung einer Einwilligung nach den Formvorschriften des BDSG.

Eine solche Differenzierung anhand des Maßstabs der Erforderlichkeit bietet sich nicht zuletzt deshalb an, weil damit auch eine datenschutzrechtliche Grundwertung des BDSG aufgegriffen wird. Nach dem BDSG bedarf es für „erforderliche" Datenübermittlungen überhaupt keiner Einwilligung, zulässig sind diese vielmehr bereits auf der Grundlage eines gesetzlichen Erlaubnistatbestands, konkret nach § 28 Abs. 1 S. 1 Nr. 1 BDSG. Letztere Vorschrift normiert an sich die bloße Selbstverständlichkeit, dass mit der Begründung eines Schuldverhältnisses auch die für die Durchführung dieses Schuldverhältnisses erforderlichen Datenverarbeitungsvorgänge legitimiert werden. Eben diese Selbstverständlichkeit muss auch für das ärztliche Behandlungsverhältnis gelten, egal ob man sich auf einen gesetzlichen Erlaubnistatbestand stützt oder auf eine entsprechende konkludente Einwilligung des Patienten.

b) Ausnahme nach § 4a Abs. 1 S. 3 BDSG

Nach der hier vorgeschlagenen Differenzierung ist also an sich eine ausdrückliche, schriftliche Einwilligung erforderlich, da die mit der Einschaltung eines Callcenters einhergehende Datenpreisgabe gerade nicht für die Erfüllung des ärztlichen Behandlungsauftrags erforderlich ist und es daher bei den Formvorgaben des BDSG bleibt. Ein Absehen vom Schriftformerfordernis kommt hier jedoch in Betracht, wenn man mit Blick auf die telefonische Kontaktaufnahme von „besonderen Umständen" i. S. des § 4a Abs. 1 S. 3 BDSG ausgeht, die hier ausnahmsweise auch eine andere (nämlich mündliche) Form der Einwilligung als „angemessen" erscheinen lassen.

Nicht verzichtbar ist hingegen die ausdrückliche Erteilung einer entsprechenden Einwilligung. Es reicht also nicht aus, dass ein Patient seine Einwilligung konkludent dadurch erteilt, dass er am Telefon bereitwillig seinen Namen und Terminwunsch gegenüber dem Callcenter offenbart. Vielmehr muss er explizit danach gefragt werden, ob er mit einer Datenaufnahme auch durch das Callcenter einverstanden ist. Dies wiederum setzt zuallererst voraus, dass dem Patienten überhaupt bewusst ist, im konkreten Fall nicht mit der Arztpraxis selbst, sondern einem externen Dienstleister zu kommunizieren. Bereits bei Entgegennahme eines Anrufs muss sich daher der externe Dienstleister deutlich als ein solcher zu erkennen geben und muss beim Patienten jeden Eindruck dahingehend vermeiden, dieser kommuniziere mit einem Mitarbeiter der Praxis selbst.

Schließlich darf die Kommunikation über ein Callcenter niemals die einzig mögliche Form der Kontaktaufnahme mit der Arztpraxis, sondern stets nur eine Ergänzung sein. Der Patient muss eine Alternative zum Callcenter haben, etwa eine direkte Verbindung zur Praxis zu anderen Zeiten oder über eine andere Nummer, andernfalls kann man von einer freiwilligen Mitteilung von Daten gegenüber einem Callcenter nicht ausgehen[44]. Nur bei einer solchen Freiwilligkeit ist aber die Einwilligung des Patienten überhaupt eine wirksame und kann die Offenbarung von Patientendaten legitimieren.

IV. Fazit

Das traditionelle Bild der Vertraulichkeit zwischen Arzt und Patient lässt sich heutzutage nur noch schwer aufrechterhalten. Die Zeiten der trauten Zweisamkeit von Arzt und Patient scheinen vorbei, stattdessen ist der ärztliche Behandlungsalltag geprägt von Informationstechnik, Arbeitsteilung und Outsourcing. Datenschutz und ärztliche Schweigepflicht müssen hierauf die richtigen Antworten finden, wobei es allerdings nicht allein darum gehen kann, einer übertriebenen Fortschrittshörigkeit („die moderne Medizin") den Weg zu bereiten. Mit datenschutzrechtlichen Regelungsprinzipien wie der Auftragsdatenverarbeitung oder der Einwilligung stehen zwar Instrumentarien bereit, mit deren Hilfe sich viele Datenverarbeitungsprozesse im Gesundheitsbereich sachgerecht regeln lassen. Woran es jedoch fehlt, ist ein Wertungsgleichklang zwischen Datenschutz und ärztlicher Schweigepflicht, insbesondere bei einer Einschaltung externer Stellen. Bestehende Widersprüche lassen sich bislang lediglich mittels punktueller Lösungsansätze auflösen, wie sie hier vorgestellt wurden. Eine „große" Lösung, wie sie insbesondere in Form einer datenschutzgesetzkonformen Fortschreibung des § 203 StGB in Betracht käme, lässt dagegen noch immer auf sich warten.

---

41) S. dazu bereits oben, sub II. 2.
42) S. soeben sub III. 2. a).
43) Vgl. *Buchner,* in: *ders.* (Hrsg.), Datenschutz im Gesundheitswesen, 2012, A/1, S. 15 f.; *Giring*, in: *Ratzel/Luxenburger* (Hrsg.), Handbuch Medizinrecht, 2. Aufl. 2011, § 15, Rdnr. 120.
44) *Menzel,* in: *Buchner* (Hrsg.), Datenschutz im Gesundheitswesen, 2012, G/2, S. 6.