OPEN ACCESS

Research Article

Datenschutz- und Medizinprodukterecht bei Ubiquitous Computing-Anwendungen im Gesundheitssektor

Data protection and medical product law with respect to medical ubiquitous computing applications

Abstract

With respect to ubiquitous computing there is a great potential of application, particularly in medicine and health care. This work deals with the legal problems which ubiquitous computing is facing in these areas. At the beginning, issues with respect to data protection and professional secrecy are treated. Afterwards the problem of applicability of medical product law for medical ubiquitous computing applications as well as the resulting requirements for manufactures, operators and users will be discussed.

Zusammenfassung

Ubiquitous Computing findet gerade in der Medizin und im Gesundheitswesen einen großen möglichen Anwendungsbereich. Diese Arbeit beschäftigt sich mit den rechtlichen Problemen, denen Ubiquitous Computing dort gegenübersteht. Im Detail werden zunächst Fragestellungen bezüglich des Datenschutzes und der Schweigepflicht behandelt und danach die Problematik der Anwendbarkeit des Medizinprodukterechts für medizinische UC-Anwendungen sowie die daraus resultieren Auflagen für die Hersteller, Betreiber und Anwender erörtert.

Hendrik Skistims[1]
Julia Zirfas[1]

1 Universität Kassel, Fachbereich Wirtschaftswissenschaften, Projektgruppe Verfassungsverträgliche Technikgestaltung, Kassel, Deutschland

1 Einleitung

Ubiquitous Computing (UC) ist ein Zusammenspiel unterschiedlicher IT-Anwendungen, die dem Nutzer seiner Situation entsprechende unterstützende Dienste zur Verfügung stellen, wobei der Nutzer oft nicht direkt, sondern lediglich implizit mit den Anwendungen interagiert [1]. Im Gesundheitswesen könnte UC beispielsweise unter anderem in der Prävention, Pflege und Diagnostik, aber auch bei der Therapie eine Rolle spielen (*Siehe auch „Ambient Assisted Living“ (AAL):* http://www.aal-deutschland.de/aal-1. *Solche Konzepte verbinden und verbessern neue Technologien und soziales Umfeld miteinander, mit dem Ziel, die Lebensqualität für Menschen in allen Lebensabschnitten zu erhöhen*). Das Hauptmerkmal der Allgegenwärtigkeit würde auch hier durch eine möglichst unauffällige Integration der Anwendung, beispielsweise in die Wohnung (Möbel) oder die Kleidung erreicht. UC-Anwendungen würden sowohl für Patienten als auch für Ärzte Fortschritte bezüglich Effizienz, Prävention und Kommunikation bieten. Außerdem könnten sie, je nach Anwendung, die Selbständigkeit und Unabhängigkeit insbesondere von älteren Menschen steigern [2].

Der Unterschied zwischen nicht medizinischen UC-Anwendungen und solchen, die zur Nutzung in der Medizin und dem Gesundheitswesen bestimmt sind, besteht in erster Linie darin, dass diese speziellen Applikationen am Menschen direkt angewendet werden. Die Funktionsfähigkeit und Zuverlässigkeit einer solchen UC-Anwendung hat somit direkte Auswirkungen auf das Wohlbefinden und die Gesundheit eines Patienten. Dementsprechend muss bei ihrer Konstruktion und dem Betreiben eine besondere Sorgfalt an den Tag gelegt werden, die im Medizinproduktegesetz Berücksichtigung findet. Außerdem werden im medizinischen Bereich nicht nur allgemeine Daten erhoben, sondern spezifische Daten, die die Gesundheit eines Menschen betreffen. Eine medizinisch genutzte UC-Anwendung würde, zusätzlich zum Standort oder den Vorlieben, außerdem beispielsweise Vitalparameter aufzeichnen, übermitteln und auch auswerten sowie eventuelle Konsequenzen ziehen. Dies erfordert einen erhöhten Grad an ständigem Vertrauen in die medizinische UC-Anwendung und die Datennutzung. Der Beitrag wird genau diese spezifischen technikrechtlichen Schwierigkeiten ansprechen, die UC im Gesundheitswesen bewältigen muss.

Im Folgenden wird zuerst ein Szenario beschrieben, das dabei helfen soll, die Möglichkeiten von UC im Gesundheitswesen zu erkennen, aber auch die rechtlichen Probleme abzuleiten. Danach beschäftigt sich das zweite Kapitel mit den Problemen und Fragestellungen bezüglich des Datenschutzes und der Schweigepflicht. Im dritten Kapitel geht es um die Anwendbarkeit des Medizinprodukterechts für medizinische UC-Anwendungen sowie

den daraus resultieren Auflagen für die Hersteller, Betreiber und Anwender. Das Fazit greift vor allem die Probleme noch einmal auf und versucht auch eine mögliche Bilanz zu ziehen über die Qualität der Vereinbarkeit von medizinischer UC-Technik mit rechtlichen Grundsätzen.

2 Szenario

Grundlage des Szenarios bildet eine UC-Anwendung, die unter anderem zum kontinuierlichen Monitoring sämtlicher Vitalparameter, wie Blutdruck, Herzfrequenz, Körpertemperatur, Atemfrequenz und Blutzucker (z.B. durch Sensoren in der Toilette) einer Person genutzt wird. Durch Bewegungssensoren könnte eine ungewöhnliche Situation, wie ein möglicher Sturz, durch das System festgestellt werden. Die Sensorik könnte in die Kleidung und Möbel integriert und somit in jeder Alltagssituation benutzt werden. Das hierfür notwendige technische Knowhow könnte durch Dienstleister aus der Informatik bereit gestellt werden. Dieser könnte zudem Anwendungen, die die Vitalparameter aufbereiten, zur Verfügung stellen und entsprechende Daten an ein Krankenhaus (spezielle Überwachungsstelle oder direkt an den behandelnden Arzt) zur Auswertung weiterleiten. Insbesondere in einer kritischen Situation soll durch das System sofort der zuständige Arzt oder, je nach Schwere des Problems, auch nur ein Angehöriger informiert werden, um eventuelle Gegenmaßnahmen einzuleiten.
Für den Fall, dass ein Patient regelmäßig Medikamente benötigt, könnte außerdem eine Benachrichtigung an den behandelnden Arzt geschickt werden, sobald der Patient ein neues Rezept für ein bestimmtes Medikament benötigt. Dies kann durch einen intelligenten Medizinschrank erfolgen, der regelmäßig Bestand, Verträglichkeit und Haltbarkeit seines Inhaltes überprüft [3]. Der Arzt unterschreibt (oder signiert mittels elektronischer Signatur) das Rezept daraufhin und legt es in einem für die UC-Anwendung abrufbaren Rezeptausgang ab. Der Patient entscheidet dann, ob das Medikament zugeschickt werden soll (das System übernimmt die Bestellung und bedient sich des gespeicherten Rezeptes) oder er es selbst abholt (in dem Fall würde das Rezept beim Betreten der Apotheke automatisch an diese übermittelt). Parallel wird eine Benachrichtigung an den Arzt geschickt, dass das Medikament abgeholt/versendet wurde und der Patient somit vorerst wieder versorgt ist. Ähnliche Möglichkeiten, beziehungsweise unterstützende Funktionen, wie zum Beispiel die Identitätsprüfung und die Hinterlegung von Patientenakten, werden sich zukünftig möglicherweise auch gerade durch die Einführung der elektronischen Gesundheitskarte und des elektronischen Rezepts eröffnen (*Siehe für weiterführende Literatur zur elektronischen Gesundheitsakte* [4]).

3 Datenschutzrecht

Im Jahre 1983 erkannte das BVerfG im sogenannten Volkszählungsurteil das Grundrecht auf informationelle Selbstbestimmung an [5]. Durch diese spezielle Ausprägung des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG sollte den neuartigen Gefährdungen, welche durch die elektronische Datenverarbeitung entstanden, begegnet werden. Im Bezug auf den medizinischen Sektor schränkt „[d]ie Weitergabe von Patientendaten [...] das Grundrecht auf informationelle Selbstbestimmung ein“ ([6], S. 98). Der Schutzbereich dieses Rechts umfasst die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ([7], § 1, Rn. 10). Insbesondere kann nicht mit personenbezogenen Daten ohne gesetzliche Grundlage, wie es das BDSG darstellt, oder aber ohne Zustimmung des Betroffenen umgegangen werde (*zum Beispiel § 67 a Abs. 1 SGB X*).

3.1 Gefährdungspotential durch Ubiquitous Computing

3.1.1 Besonderheiten des Gesundheitswesens

Der Patient befindet sich aufgrund der aus den medizinischen Zusammenhängen resultierenden Komplexität in einem besonderen Abhängigkeitsverhältnis zum Arzt ([8], S. 24). Hieraus ergibt sich zwischen Arzt und Patient ein besonderes, das Behandlungsverhältnis charakterisierendes, Vertrauensverhältnis, dessen Schutz maßgeblich für die Heilungschancen eines Patienten ist ([9], S. 633). Dieses spiegelt sich insbesondere in dem durch die Berufsordnungen statuierten Grundsatz der Pflicht zur persönlichen Behandlung wieder ([10], S. 14). Die räumliche Trennung, welche die im Szenario dargestellte UC-Anwendung unweigerlich zur Folge hätte, beinhaltet über die konventionellen Methoden hinausgehende Risiken, auch datenschutzrechtlicher Art ([11], S. 143).
Ein weiterhin zu beachtender Umstand ist die besondere Qualifikation der Leistungserbringer (*Der Begriff des Leistungserbringers ist weit zu verstehen. Er umfasst jede Person, die die Verhütung von Krankheiten gem. §§ 20–24 SGB V, die Früherkennung §§ 24 a, 24 b, 25, 26 SGB V, sowie die Krankenbehandlung gem. § 27 SGB V vornimmt*) ([12], S. 168), welche wiederum an die besondere Art der Leistung, die sie erbringen, geknüpft ist ([8], S. 25). Im Rahmen telematischer und ubiquitärer Anwendungen, welche den Grundsatz der persönlichen Behandlung nicht erfüllen, ist eine besondere Gewähr für das tatsächliche Bestehen jener Qualifikation bei der Verarbeitung der medizinischen Daten bereitzustellen. Eine denkbare Möglichkeit zur Erfüllung der Authentizität wäre die Ausstattung des Systems mit einer qualifizierten elektronischen Signatur. Durch die Möglichkeit sogenannter Attribut-Zertifikate gem. § 7 Abs. 2 SigG, in welchen entsprechende Attribute niedergelegt werden könnten, ist die Möglichkeit gegeben, die besondere Qualifikation des Leistungserbringers zu gewährleisten ([4], S. 322).

Das System müsste demnach sicherstellen, dass die erhobenen Daten nur an Empfänger weitergeleitet werden, welche die zuvor definierten Attribute erfüllen.

3.1.2 Arten der erhobenen Daten

Auch die Art, der durch UC erhobenen Daten, gibt Anlass für ein genaueres Hinsehen. Besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG unterstehen besonderen Restriktionen. Diese schlagen sich vor allem in den besonderen Anforderungen der Eingriffsvoraussetzungen nieder. Art. 8 Abs. 1 95/46/EG (*Richtlinie 45/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*) gibt genau diesen Datenkatalog wieder ([4], S. 275) und konstatiert damit die Verpflichtung der Mitgliedsstaaten, die Verarbeitung dieser Art von personenbezogenen Daten grundsätzlich zu verbieten.
Bereits die Information, dass überhaupt Arztbesuche stattgefunden haben, kann in den Anwendungsbereich des § 3 Abs. 9 BDSG fallen ([7], § 3, Rn 56). Sollten Krankendaten über Telematische Systeme an Leistungserbringer gesendet werden, ist zudem Art. 10 Abs. 1 GG zu beachten. Der Fernmeldeverkehr umfasst jede fernmeldetechnisch übermittelte Übertragung von Informationen an individuelle Empfänger ([13], Art. 10, Rn. 39). In jedem Falle würde der Umstand, dass vorliegend eine Kommunikation zwischen Computern stattfindet, die Schutzbereichseröffnung nicht ausschließen ([14], S. 273). Des Weiteren unterstehen sämtliche Angaben zur Gesundheit eines Menschen dem Anwendungsbereich des § 3 Abs. 9 BDSG. Wie in dem Szenario angedeutet, können im Rahmen eines kontinuierlichen Monitoring des Patienten umfangreiche Datenbestände hinsichtlich seiner Vitalfunktionen generiert werden. Die in dem Szenario zugrunde gelegten Datenverarbeitungsvorgänge haben somit personenbezogene medizinische Informationen zum Inhalt, die als besonders sensitiv im Sinne des § 3 Abs. 9 BDSG einzustufen sind. Hieraus ergibt sich die besondere Verpflichtung eines ausdrücklichen Hinweises auf diese Art der Daten im Rahmen der Erteilung einer Einwilligung gemäß § 4a Abs. 3 BDSG, sowie besondere Regelungen hinsichtlich der Erhebung, Verarbeitung und Nutzung in § 13 Abs. 2, sowie in § 28 Abs. 6-9 BDSG.

3.2 Ubiquitous Computing, Medizin und der Datenschutz

3.2.1 Die Einwilligung

Der Umgang mit personenbezogenen Daten ist solange verboten, wie er nicht gesetzlich ausdrücklich zugelassen ist oder aber eine Einwilligung des Betroffenen besteht ([15], Kap. 4.8, Rn. 3). Dieses bedeutet zunächst, dass die Einwilligung solange unerheblich ist, wie der Umgang mit den personenbezogenen Daten sowieso gesetzlich zugelassen ist ([16], § 4, Rn. 6). Eine Erhebung oder Übermittlung von Daten an die Krankenkassen ist von §§ 67 Abs. 5 SGB X und 67 a Abs. 1 SGB X für die in 284 Abs. 1 SGB V konkretisierten Zwecke gedeckt. Soweit es jedoch um den Umgang mit Daten durch den Leistungserbringer im Rahmen von UC-Anwendungen geht, greifen diese Normen nicht, da sie die Rechtsbeziehungen zwischen Leistungserbringer und gesetzlichen Krankenkassen betreffen. Eine Einwilligung wäre folglich erforderlich. Im Rahmen eines dauernden Behandlungsverhältnisses ist es möglich, die Einwilligung vorher schriftlich zu fixieren. Auch die Einbettung der Einwilligung in die Technik selbst, mittels Delegation an einen Client, ist ein gangbarer Weg ([17], S. 74; [18], S. 629). Angesichts der Vielzahl der Datenverarbeitungs- und Erhebungsvorgänge, welche aus der Omnipräsenz der Sensorik resultiert, besteht das rein praktische Problem, wie bestimmt die Einwilligung zu sein hat ([19], S. 136 ff.). Grundsätzlich hat sich eine Einwilligung auf einen genau beschriebenen Verwendungszusammenhang zu beziehen ([16], § 4, Rn. 77). Gerade vor dem Hintergrund ubiquitärer, sich selbst adaptierender Systeme wird eine sogenannte relative Unvollständigkeit der Einwilligung jedoch wohl nicht zu vermeiden sein ([16], § 4, Rn. 80; [19], S. 136 ff.). Dieses gilt umso mehr als gerade im medizinischen Bereich unvorhergesehene Situationen eintreten können, die ein sofortiges Einschreiten notwendig machen. Um ein gewisses Maß an Bestimmtheit zu erreichen, wird mindestens die Angabe des Behandlungszweckes zu fordern sein. Um eine am Einzelfall orientierte Beurteilung vornehmen zu können, wäre es zudem hilfreich, die Ziele der Verarbeitung und auch deren einzelne Phasen in die Einwilligung mit aufzunehmen ([16], § 4, Rn. 80).
Probleme könnten auch hinsichtlich der Kostenübernahme durch die gesetzlichen Krankenkassen entstehen. Die Kosten einer Behandlung wäre schon allein durch Telemedizin gegenüber herkömmlicher Behandlungsmethoden um bis zu 38% (*Laut einer von der Europäischen Union in Auftrag gegebenen Studie von „Health Service24", abrufbar unter:* http://www.healthservice24.com/Internet/external/healthservice24/images_/D1.5_HS24%20Final%20Report.pdf *(zuletzt abgerufen am 10.11.2010), S. 5*) senkbar. Die Einführung flächendeckender ubiquitärer Elektronik im medizinischen Bereich wäre somit, zumindest wenn es um die Überwachung der Vitaldaten eines Patienten geht, die kostengünstigere Alternative zu stationären Aufenthalten. Fraglich erscheint somit, inwiefern die Krankenkassen zur Ablehnung der Kostenübernahme von konventionellen Behandlungsmethoden nach dem in § 12 Abs. 1, HS. 1 SGB V manifestierten Wirtschaftlichkeitsgebot berechtigt sind, wenn durch UC günstigere Alternativen zur Verfügung stehen. Nach dem Wirtschaftlichkeitsgebot ist nur jene Leistung erstattungsgeeignet, bei der das günstigste Verhältnis zwischen Aufwand und Wirkung besteht ([20], § 12, Rn. 40). Dieses Problem wird jedenfalls dann virulent, wenn Patienten eine entsprechende Erhebung und Verarbeitung ihrer Gesundheitsdaten ablehnen und eine „teurere" konventionelle Behandlung vorziehen. An die Verweige-

rung der Einwilligung im Sinne des § 4a Abs. 1 BDSG dürfen jedoch keine nachteiligen Folgen für den Berechtigten geknüpft werden ([15], Kap. 4.8, Rn. 54). Mittelbare Folge der Ablehnung der Einwilligung wäre somit die datenschutzrechtliche Unzulässigkeit des Monitoring, wodurch zwangsweise nur noch konventionelle und somit teurere Methoden in Betracht kämen. Würde es den Krankenkassen in diesen Fällen gestattet werden, die Ablehnung der Kostenübernahme mit dem Wirtschaftlichkeitsgebot aus § 12 Abs. 1, HS. 1 SGB V zu begründen, hätte dieses weitreichende Folgen für die Informationelle Selbstbestimmung der Berechtigten. Es würde zu einem Zielkonflikt zwischen der Verwirklichung des Sozialstaatsprinzips aus Art. 20 Abs. 1 GG und der Informationellen Selbstbestimmung kommen (*Vgl. auch zur öffentlichen Wahrnehmung dieses Problems:* http://www.focus.de/gesundheit/ratgeber/zukunftsmedizin/visionen/tid-18376/medizin-glaesern-und-gesund_aid_504061.html *(zuletzt abgerufen am 27.5.2010)*).

3.2.2 Transparenz

Der Grundsatz der Transparenz erfordert, dass die Daten direkt beim Betroffenen zu erheben sind und er vor dem Umgang mit seinen persönlichen Daten zu unterrichten ist ([19], S. 133). Insbesondere Letzteres hat das Ziel, dem Betroffenen alle Informationen an die Hand zu geben, die zur Abschätzung des Anlasses, Zieles und Folgen der Verarbeitung notwendig sind ([15], Kap. 4.8, Rn. 48). Dieser Schutzzweck erscheint nur schwer mit einer etwaigen relativen Unbestimmtheit der Einwilligung vereinbar zu sein. Zu beachten ist jedoch, dass ubiquitäre Systeme gerade dazu bestimmt sind, unmerklich im Hintergrund zu agieren, um den Patienten zu unterstützen bzw. seine Vitaldaten zu überwachen ([21], S. 208). Würde trotz der Vielzahl der datenverarbeitenden Vorgänge eine vollumfängliche Aufklärung hinsichtlich jedes Verarbeitungsvorganges gefordert werden, wäre dieses dem Schutzzweck der Transparenz nicht zuträglich. Die eigentlich bezweckte selbstbestimmte Wahrnehmung der Rechte des Betroffenen würde das Gegenteil von Sensibilität erreichen ([19], S. 134). Ein denkbarer Kompromiss wäre es, die Informationspflichten auf Strukturinformationen über die Systeme abzielen zu lassen ([19], S. 134). Mit einem solchen Wissen würde es dem Berechtigten grundsätzlich selbst ermöglicht werden, sich über die tatsächliche und rechtliche Tragweite seiner Einwilligung klar zu werden.
Weiterhin ist an etwaige Dokumentationspflichten der Leistungserbringer zu denken. Soweit schon die medizinisch indizierte Videoüberwachung (Monitoring) als Teil der Behandlung anzusehen ist ([22], S. 81), hat der Leistungserbringer sämtliche elektronische Aufzeichnungen der Krankenakte beizufügen. Selbiges ist aus einem Erst-Recht-Schluss auch für die Behandlung im Rahmen ubiquitärer telematischer Verfahren zu fordern.

3.2.3 Die Schweigepflicht

Die ärztliche Schweigepflicht ergibt sich aus ärztlichem Standesrecht und § 203 StGB ([6], S. 98). Aus Letzterem geht hervor, dass wer „unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Arzt, (...) anvertraut worden oder sonst bekanntgeworden ist“, mit Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft wird. Die Schweigepflicht umfasst somit alle Tatsachen, die dem Arzt im Rahmen seiner beruflichen Eigenschaft bekannt geworden sind ([23], § 5, Rn. 121). Von der Schweigepflicht umfasst sind somit auch sämtliche Krankendaten, die im Rahmen ubiquitärer Verfahren erhoben werden.
Fraglich erscheint somit, inwiefern sich die Schweigepflicht auf das im Szenario angelegte Verhältnis zwischen Krankenhaus und externem Dienstanbieter auswirkt. Ein Krankenhaus wird weder ein originäres Interesse daran haben, noch die technischen und personellen Möglichkeiten zur Kreation und Wartung einer eigenen EDV-Infrastruktur besitzen. Die Integration externer Dienstleister im EDV-Bereich wird somit aus rein wirtschaftlichen Erwägungen bei UC den Regelfall darstellen. Die rechtlichen Fragen knüpfen an die konkrete Ausgestaltung einer solchen Infrastruktur an. Übermittelt der Dienstanbieter ohne weitere Zwischenschritte die erhoben Krankendaten direkt an das Krankenhaus weiter, bestehen zunächst weniger Bedenken hinsichtlich der Verletzung der Schweigepflicht. Wie sollen jedoch Krankenhaus und Dienstanbieter miteinander abrechnen, wenn Letzterem keine Abrechnungsgrundlage zur Verfügung steht? Eine anonymisierte Erhebung der Daten wäre denkbar, jedoch faktisch wohl kaum möglich. Jedenfalls würde dem Dritten immer eine Möglichkeit, wenigstens zur Re-Individualisierung, verbleiben.
Eine Offenbarung der Daten wäre jedoch lediglich strafbar, wenn diese in unbefugter Weise geschehen würde. Die Befugnis zur Offenbarung ergibt sich entweder aus einer Rechtsvorschrift oder aber aus der Einwilligung des Betroffenen. Zweifelhaft erscheint, ob das Datenschutzrecht eine solche Befugnis zur Offenbarung gibt. Teilweise wird vertreten, es stehe grundsätzlich neben dem Strafrecht ([6], S. 99), habe also keine Auswirkung auf eine etwaige Befugnis. Anders sei dieses nur, wo über das Recht hinaus eine Pflicht zur Übermittlung von Daten konstituiert ist, wie in §§ 294 ff. SGB V ([24], § 203, Rn. 29). §§ 294 ff. SGB V scheiden jedoch aus, da diese lediglich das Verhältnis von Leistungserbringer und gesetzlichen Krankenkassen regeln. In Betracht zu ziehen wäre zudem § 28 Abs. 1, S. 1, Nr. 1 BDSG, allerdings nur für die Fälle, in denen der Patient ein originäres Vertragsverhältnis zum externen Dienstanbieter unterhält. Auch dieses ist jedoch unwahrscheinlich. Der Patient begibt sich zur Behandlung einer Krankheit in die Hände eines Arztes, nicht in die eines Informatikers. Auch die Abtretung der Ansprüche des Krankenhauses gegen einen Dritten ohne Einwilligung des Betroffenen erfüllt den Tatbestand des § 203 Abs. 1, Nr. 1 StGB und ist darüber hinaus gem.

§ 134 BGB nichtig ([25], S. 184; *So auch: BGH NJW 1991, S. 2955*). Letztlich verbleibt nur noch die Möglichkeit einer Einwilligung des Patienten, um ein unbefugtes Übermitteln von Daten i.S.d. § 203 StGB zu vermeiden.
Zu beachten ist, dass es sich bei der Beauftragung eines externen Dienstleisters zur Datenerhebung, Verarbeitung und Nutzung um eine sog. Funktionsübertragung handelt ([22], S. 81). Es handelt sich demnach jedenfalls bei der im Szenario zugrunde gelegten Situation um eine Auftragsdatenverarbeitung i.S.d. § 11 BDSG. Der Auftraggeber, mithin das Krankenhaus, bleibt somit verantwortliche Stelle i.S.d. § 3 Abs. 8 BDSG in allen Rechtsbeziehungen, d.h. sowohl gegenüber öffentlichen Stellen, als auch gegenüber dem Betroffenen ([16], § 11, Rn. 40). Eine solche Beauftragung ist jedenfalls nur zulässig, soweit das jeweilige landesspezifische Krankenhausgesetz diese gestattet *(Vgl.: Art. 27 Abs. 4, S. 5 BayKrG*). Wie bereits oben angedeutet, ist die Einbindung entsprechender externer, zur Abrechnung befugter Stellen lediglich dann zulässig, wenn eine explizite oder inzidente Einbindung von der Schweigepflicht vorliegt ([26], S. 730; *Vgl. auch: BGH, NJW 1991, S. 2955; OLG Düsseldorf, DSB 10/97, S. 17*). Dieses bedeutet sowohl die eindeutige Unterrichtung des Patienten, als auch seine Möglichkeit zum Widerspruch.
Übermittelt die zur Behandlung berufene Person Daten in die Sphäre des Patienten, welche Rückschlüsse auf seinen gesundheitlichen Zustand erlauben, so ist sicherzustellen, dass diese Daten nicht an unberechtigte Dritte gelangen. Das technische System müsste somit in einer Weise konfiguriert werden, dass die Vitaldaten nur an Empfänger übermittelt werden, welche authentifiziert wurden. Hierzu wäre die Nutzung von qualifizierten elektronischen Signaturen (§ 2, Nr. 3, a.) SigG) eine denkbare Methode. Dabei wird der Absender einer E-Mail durch eine solche digitale Signatur identifiziert. Zur Lösung des vorliegenden Problems könnte beispielsweise der Patient eine Anfrage an den betreffenden Arzt schicken, die mit einer qualifizierten elektronischen Signatur versehen ist und ihn als den richtigen Patienten ausweist. Daraufhin kann der Arzt auf diese antworten. Zur vollen Verwirklichung des eigentlichen Gestaltungszieles im Bezug auf UC müsste die Signatur und deren Überprüfung jedoch unabhängig von einem persönlichen Handeln, infolge eines lediglich initiierten automatischen Prozesses von statten gehen. Dieser Umstand schließt die Anerkennung als qualifizierte elektronische Signatur im Sinne des § 2 SigG jedoch nicht per se aus ([27], S. 138). Des Weiteren sollten die Daten immer nur verschlüsselt übertragen werden.

4 Medizinprodukte

Das Nicht- oder Fehlfunktionieren von Anwendungen, wie im oben dargestellten Szenario, könnte sich gefährlicher als bei nicht medizinischen UC-Anwendungen darstellen. Aus diesem Grund greift bei solchen Anwendungen mit erhöhtem Sicherheitsinteresse das Medizinprodukterecht, welches garantiert, dass ein bestimmter Sicherheitsstandard bei der Herstellung und der Verwendung eingehalten wird.
Das deutsche Medizinproduktegesetz entstand aufgrund der Umsetzungspflicht der „Harmonisierungsrichtlinien“ zur Vereinheitlichung und Sicherung eines europäischen Medizinprodukterechts (*Dies sind die Richtlinie 93/42/EWG des Rates vom 14.06.1993 über Medizinprodukte, die Richtlinie 98/42/EG über In-vitro-Diagnostika sowie die Richtlinie 90/385/EWG zur Angleichung der Rechtsvorschriften über aktive implantierbare medizinische Geräte*) und trat am 1. Januar 1995 in Kraft. Der grundsätzliche Zweck des Medizinproduktegesetzes (MPG) ist es, „den Verkehr mit Medizinprodukten zu regeln und dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritter zu sorgen“. Das Gesetz und seine Verordnungen richten sich an Hersteller, Betreiber und Anwender medizinisch technischer Geräte.

4.1 Klassifizierung von Ubiquitous Computing als Medizinprodukt

Eine UC-Anwendung, die unter anderem zur medizinischen Überwachung oder Behandlung von Krankheiten dient, ist unter Umständen als Medizinprodukt zu klassifizieren. Dies würde zahlreiche Auflagen und Pflichten nach sich ziehen. Medizinprodukte sind gemäß § 3 Nr. 1 MPG alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke

a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,

b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen, [...]

zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird (*Deren Wirkungsweise kann aber durch solche Mittel unterstützt werden*).
Eine Ausnahme bieten hierbei lediglich Sonderanfertigungen (*§ 3 Nr. 8 MPG*). Auch wegen des erheblichen Entwicklungsaufwandes sind UC-Anwendungen in den meisten Fällen eher dazu vorgesehen, nach der Forschung- und Entwicklungsphase bei einer größeren Masse von Patienten angewendet zu werden. Das Medizinproduktegesetz schließt solche serienmäßig hergestellten Medizinprodukte von der Regelung der Sonderanfertigung aus. Eine UC-Anwendung, die nicht speziell nur für die Verwendung durch einen spezifischen Patienten pro-

duziert wurde, ist demnach als Medizinprodukt zu klassifizieren (*Weiterhin ist ein Medizinprodukt ein Produkt, das dazu bestimmt sind, Arzneimittel im Sinne des § 2 I AMG zu verabreichen. Im Gegensatz dazu sind gemäß § 2 Abs. 4 MPG Arzneimittel, kosmetische Mittel, Transplantate oder persönliche Schutzausrüstungen keine Medizinprodukte*). Es stellt sich die Frage, ob sich die Kategorisierung als Medizinprodukt sofort auf eine ganze UC-Anwendung bezieht oder nur auf den Teil der tatsächlich im Kontakt zum Patienten steht. Nach strenger Auslegung des Gesetzeswortlautes wäre eher nicht die gesamte, im Szenario beschriebene, UC-Anwendung ein Medizinprodukt, sondern lediglich der Teil, der auch wirklich zum Zwecke der Erkennung, Verhütung, Überwachung, Behandlung und Linderung von Krankheiten dient.
Nichtsdestotrotz können weitere Teile der UC-Anwendung als Medizinproduktezubehör kategorisiert werden. Zubehör für Medizinprodukte sind gemäß § 3 Nr. 9 MPG, „Gegenstände, Stoffe sowie Zubereitungen aus Stoffen, die selbst keine Medizinprodukte (...) sind, aber vom Hersteller dazu bestimmt sind, mit einem Medizinprodukt verwendet zu werden, damit dieses entsprechend der von ihm festgelegten Zweckbestimmung des Medizinproduktes angewendet werden kann“. Die Messung der Vitalfunktion wird im Szenario durch Sensoren durchgeführt. Jeder davon stellt ein Medizinprodukt im Sinne des MPG darstellen. Kleidung und Möbel, in die diese Sensorik integriert ist, würden eher als Zubehör gelten, denn sie erkennen nicht selbst Krankheiten oder Abweichungen der Vitalwerte, ermöglichen aber als Träger der Sensorik deren Benutzung. Zubehör wird gemäß § 2 Abs. 1 MPG als eigenständiges Medizinprodukt behandelt ([28], Vorwort).

4.2 Richtlinien für Hersteller

4.2.1 CE-Kennzeichen und grundlegende Anforderungen

Ein Medizinprodukt wird zuerst vom Hersteller in den Verkehr gebracht und dann vom Betreiber oder dem Anwender in Betrieb genommen (*Gemäß § 3 Nr. 11 MPG ist das Inverkehrbringen jede entgeltliche oder unentgeltliche Abgabe von Medizinprodukten an andere*). Hersteller ist gemäß dem § 3 Nr. 15 MPG jede natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung und Kennzeichnung eines Medizinproduktes im Hinblick auf das erstmalige Inverkehrbringen im eigenen Namen verantwortlich ist. Entscheidend für den Begriff des Herstellers ist demnach in erster Linie, wer die Zweckbestimmung festlegt und das Produkt unter seinem Namen in den Verkehr bringt, nicht, dass er es tatsächlich hergestellt hat ([29], S. 46). Diese Zweckbestimmung muss objektiv nachvollziehbar sein und wird durch Produktbeschreibung oder Werbung verbreitet.
In der Regel dürfen gemäß § 6 Abs. 1 MPG Medizinprodukte in Deutschland nur in den Verkehr gebracht werden, wenn sie mit einer CE-Kennzeichnung versehen sind (*Davon ausgenommen sind lediglich die schon angesprochenen Sonderanfertigungen, eigenhergestellte und -benutzte Produkte, Medizinprodukte zur klinischen Prüfung, befristet zugelassene Medizinprodukte oder In-vitro-Diagnostika, die für Leistungsbewertungszwecke bestimmt sind*). Ansonsten sind sie nicht zulässig. Damit deklariert der Hersteller, dass er die Anforderungen der europäischen Normen an Qualität und Sicherheit für den Patienten, den Anwender und auch für Dritte erfüllt. Voraussetzung für diese Kennzeichnung ist unter anderem, auch für UC, das im Gesundheitswesen eingesetzt wird, dass es die grundlegenden Anforderungen an Medizinprodukte einhalten muss. Diese ergeben sich gemäß § 7 MPG unter anderem aus Anhang I der Richtlinie (*Richtlinie 93/42/EWG (ABl. L 169 vom 12.7.1993, S. 1), die zuletzt durch Artikel 2 der Richtlinie 2007/47/EG (ABl. L 247 vom 21.9.2007, S. 21) geändert worden ist. Weitere Anforderungen finden sich beispielsweise für aktive implantierbare Medizinprodukte im Anhang 1. der Richtlinie 90/385/EWG des Rates vom 20. Juni 1990 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über aktive implantierbare medizinische Geräte (ABl. L 189 vom 20.7.1990, S. 17), die zuletzt durch Artikel 1 der Richtlinie 2007/47/EG (ABl. L 247 vom 21.9.2007, S. 21) geändert worden ist sowie für In-vitro-Diagnostika im Anhang I der Richtlinie 98/79/EG*) über Medizinprodukte. Außerdem muss ein jeweiliges Konformitätsbewertungsverfahren durchgeführt werden [30]. Der Hersteller ist daraufhin verantwortlich und haftet auch dafür, dass die CE-Kennzeichnung eines Produktes hält, was sie verspricht [30].
Hervorgehend aus den grundlegenden Anforderungen, müssen die Produkte so ausgelegt und hergestellt werden, dass ihre Anwendung weder den klinischen Zustand und die Sicherheit der Patienten, noch die Sicherheit und die Gesundheit der Anwender oder gegebenenfalls Dritter gefährdet, wenn sie unter den vorgesehenen Bedingungen und zu den vorgesehenen Zwecken eingesetzt werden. Etwaige Risiken müssen, verglichen mit der nützlichen Wirkung für den Patienten, vertretbar und mit einem hohen Maß des Schutzes von Gesundheit und Sicherheit vereinbar sein. Auch die weiteren grundlegenden Vorschriften dienen auf unterschiedliche Weise alle diesem übergeordneten Ziel der Risikominimierung. Zusätzlich ist der Hersteller oder eine dazu befugte Person, die im Einvernehmen mit dem Hersteller handelt, dafür verantwortlich, ein Medizinprodukt am Betriebsort einer Funktionsprüfung zu unterziehen und eine vom Betreiber beauftragte Person anhand der Gebrauchsanweisung sowie beigefügter sicherheitsbezogener Informationen und Instandhaltungshinweise in die sachgerechte Handhabung, Anwendung und den Betrieb des Medizinproduktes sowie in die zulässige Verbindung mit anderen Medizinprodukten, Gegenständen und Zubehör einzuweisen (§ 5 Abs. 1 MPBetreibV). Problematisch für den Hersteller wird dabei die Anforderung sein, dass eine Funktionsprüfung am Betriebsort vorgeschrieben ist. Damit ist eine technische bzw. automatische Kontrolle des Systems getrennt vom Betriebsort ausgeschlossen.
Das MPG selbst enthält keine Haftungsregeln. Für den Hersteller gilt aber das Produkthaftungsgesetz mit einer

Fehlerhaftung nach Art der Gefährdungshaftung (§ 1 Produkthaftungsgesetz) ([12], S. 792). Unter der Voraussetzung, dass der Betreiber und Anwender ein Medizinprodukt nur nach seiner Zweckbestimmung einsetzt und trotzdem etwas passiert, haftet der Hersteller demnach im Rahmen der von ihm festgelegten Zweckbestimmung. Des Weiteren gelten die §§ 823 ff. BGB ([29], in § 22). Die Nichteinhaltung von Regelungen aus dem MPG kann für Hersteller, Betreiber und Anwender nach den §§ 40–42 MPG zudem mit einer Freiheitsstrafe bestraft werden.

4.2.2 Einteilung von Medizinprodukten in Risikoklassen

Wie ein Konformitätsverfahren bei einem Medizinprodukt durchgeführt werden muss, hängt davon ab, zu welcher Risikoklasse das Medizinprodukt zuzuordnen ist. Nach § 13 Abs. 1 MPG i.V.m. Art. 9 Abs. 1 der Richtlinie 93/42/EWG gibt es vier Risikoklassen, in die die Produkte anhand ihres Gefährdungspotentials eingeordnet werden (*Die genaue Einordnung erfolgt nach den 18 Klassifizierungsregeln des Anhangs IX dieser Richtlinie*). Die im UC verwendeten Medizinprodukte können oftmals in die ersten beiden Klassen (Klasse I und IIa) eingeordnet werden. Das sind Produkte mit geringem bzw. mittlerem Risikopotential. Bei Produkten der Klasse I liegt die Verantwortung eines Konformitätsverfahrens allein beim Hersteller (Selbstzertifizierung). Ab der Klasse II ist es notwendig, eine Zertifizierungsstelle hinzuzuziehen (benannte Stelle). Diese überprüft dann, ob das Produkt mit den grundlegenden Anforderungen übereinstimmt und stellt eine Bescheinigung aus, die dem Hersteller erlaubt die CE-Kennzeichnung anzubringen. Die Regelungen dazu und die Einordnung von Produkten in die Risikoklassen wurde zu Beginn des Jahres 2010 durch eine Novelle des MPG (*BGBL 2009, Teil I Nr. 48, S. 2326*) weiter verschärft. Produkte, die Software enthalten oder bei denen es sich um medizinische Software handelt, müssen nun beispielsweise im Rahmen des Konformitätsbewertungsverfahrens validiert werden.

4.3 Richtlinien für Anwender und Betreiber

Die Richtlinien für Anwender und Betreiber ergeben sich in erster Linie aus der Medizinproduktebetreiberverordnung (MPBetreibV). Diese Verordnung wurde auf Grundlage der Ermächtigungsgrundlage aus § 37 Abs. 5 Nr. 1 MPG erlassen und legt Anforderungen an das Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten, die zu gewerblichen und wirtschaftlichen Zwecken dienen, fest.
Danach dürfen Medizinprodukte nur von Personen errichtet, betrieben, angewendet und in Stand gehalten werden, die dafür die erforderliche Ausbildung oder Kenntnis und Erfahrung besitzen. Demzufolge dürfen Betreiber eines Medizinproduktes auch nur Personen mit dem Errichten und Anwenden von Medizinprodukten beauftragen, die die vorgenannte Voraussetzung erfüllen. Gleichzeitig hat sich der Anwender vor der Anwendung eines Medizinproduktes von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand des Medizinproduktes zu überzeugen und die Gebrauchsanweisung sowie die sonstigen beigefügten sicherheitsbezogenen Informationen und Instandhaltungshinweise zu beachten.
Daraus ergibt sich das Problem, dass es durch die Ubiquität der im Szenario beschriebenen Anwendungen nicht immer eindeutig ist, wer in diesem konkreten Fall Anwender, beziehungsweise Betreiber ist. Keiner der beiden Begriffe ist im Medizinproduktegesetz oder der Betreiberverordnung näher definiert. Es ergibt sich aber, auch im Zusammenhang mit den Grundsätzen bezüglich Eigentum und Besitz des Bürgerlichen Gesetzbuches, dass ein **Betreiber** diejenige natürliche oder juristische Person ist, die das Medizinprodukt besitzt, also die Sachherrschaft darüber hat [31]. Beispiele für Betreiber können Träger eines Krankenhauses oder auch ein Arzt als Inhaber einer Arztpraxis sein. Ein **Anwender** ist die Person, die eigenverantwortlich über die Anwendung des Medizinproduktes entscheidet und dieses auch tatsächlich am Patienten anwendet und zwar unabhängig von seiner Qualifikation ([31], S. 47). Darum könnte beispielsweise auch der Patient Anwender sein ([31], S. 47).
Nach Betrachtung der beiden Begriffe kann die Schlussfolgerung gezogen werden, dass zwar unter bestimmten Umständen der Patient selbst Anwender ist, aber dennoch zu beachten ist, dass die UC-Anwendungen sich in den meisten Fällen „selbst anwenden“ und eben gerade nicht die Interaktion des Patienten erwartet wird. Wenn man annimmt, dass der Patient als Anwender gilt, stellt sich weiterhin die Frage, was unternommen werden muss, damit er die in § 2 Abs. 2 MedBetreibV geforderte Ausbildung oder Kenntnis und Erfahrung erlangt, um das Produkt anzuwenden. Die Frage ist auch, ob speziell alte und kranke Menschen, für die diese UC-Anwendungen gedacht sind, in der Lage sind, sich selbst von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand der Anwendung zu überzeugen, wie es beispielsweise in § 2 Abs. 5 MPBetreibV gefordert wird. Die UC-Anwendung ist im Zweifelsfall wohl auch zu kompliziert gestaltet, um hier eine Funktionsfähigkeit durch den Anwender festzustellen. Demnach wäre es notwendig, entweder eine einfache Möglichkeit zur Überprüfung in die UC-Anwendung zu integrieren oder für entsprechende Anwendungen eine gesetzliche Regelung zu finden, die es dem Hersteller ermöglicht das System über automatisierte Berichte regelmäßig zu überprüfen. Klar ist bei einer ubiquitären Anwendung auch, dass sie nicht einfach einen An/Aus-Schalter besitzt. Resultierend daraus müssten gesetzlich feste Überprüfungsrhythmen festgelegt werden, statt der von der Betreiberverordnung vorgesehen Überprüfung „vor der Anwendung eines Medizinproduktes“.
Gleichzeitig ist auch schwierig einzuordnen, wer der Betreiber ist. Nach bisheriger Ansicht wird eine UC-Anwendung wahrscheinlich eher selten von einem Arzt erworben und Patienten zur Verfügung gestellt. Möglicherweise wird es aber in Zukunft tatsächlich so sein, dass Kranken-

kassen die Verwendung solcher Anwendungen als kostengünstigere Alternative zu einem Krankenhausaufenthalt sehen und daraufhin die Anwendung den Patienten zur Verfügung stellen. In diesem Fall wäre die Krankenkasse wohl am ehesten als Betreiber anzusehen. In den sonstigen Fällen interagiert die Anwendung, als allgegenwärtiger Dienst, direkt mit dem Patienten ohne Zwischenstufe. Das System steuert sich in gewisser Weise selbst, so dass der Patient nicht immer direkten Einfluss auf die Geschehnisse hat, geschweige denn es manuell bedient, wie es die bisherige Kategorisierung im Auge hatte. Der Betreiber wäre im besten Falle derjenige, der für das Funktionieren der gesamten UC-Anwendung sorgt und diese betreibt, was aber bedeuteten würde, dass dieser auch alle an ihn gestellten Richtlinien zu befolgen und auszuführen hat. Dies ist sicherlich nicht die Intention der UC-Diensteanbieter und bietet daher ein enormes Abschreckungspotential für die Implementierung solcher medizinischer Funktionen in deren Anwendungen.
Zudem wird festgelegt, dass der Anwender vor der Anwendung eines Medizinproduktes die Gebrauchsanweisung sowie die sonstigen beigefügten sicherheitsbezogenen Informationen und Instandhaltungshinweise zu beachten hat. Im speziellen ist es fraglich, ob ältere und kranke Leute eine solche Gebrauchsanweisung überhaupt lesen möchten oder können oder es sie möglicherweise sogar von der Benutzung abschreckt (*Oft werden sich UC-Anwendungen aktiver Medizinprodukte bedienen. Ein aktives Medizinprodukt liegt vor, wenn der Betrieb des Produktes von einer Energie- oder Stromquelle abhängt (§ 13 MPG verweist für die Definition des aktiven Medizinproduktes auf den Anhang IX der Richtlinie 93/42/EWG). Das führt dazu, dass hierfür weitere Vorschriften zu beachten sind. (§§ 6-9 MPBetreibV)*).
Durch die Schwierigkeit der Umsetzung der gesetzlichen Anforderungen kann geschlossen werden, dass viele Ansätze des UC im Widerspruch zu Forderungen stehen, die bei der Zertifizierung und Anwendung eines Medizinprodukts gestellt werden, insbesondere da hier alle möglichen Betriebsfälle eines Produktes beschrieben und getestet werden müssen (So auch: [2]).

5 Fazit

Der Einsatz von UC-Anwendungen verspricht für das Gesundheitswesen große Erleichterungen und Verbesserungen. Jedoch konnte gezeigt werden, dass einige praktische Anwendungsprobleme existieren, sowohl im Datenschutz als auch im Medizinprodukterecht.
Es sind aufgrund der Sensibilität der Daten strenge Anforderungen an die Einwilligung einzuhalten. Die Anforderungen an die Informationspflichten sind durch Strukturinformationen wenigstens zu ergänzen. Es wird darauf zu achten sein, dass UC-Anwendungen nicht dazu führen, dass Gesundheit nur um den Preis der Informationellen Selbstbestimmung zu erhalten ist. UC-Anwendungen werden wohl nur durch eine Auftragsdatenverarbeitung umsetzbar sein. Eine solche ist vor dem Hintergrund der besonderen Sensibilität und des besonderen Vertrauensverhältnisses zwischen Arzt und Patient aber problematisch und somit durch eine Einwilligung des Patienten abzusichern.
Bei Medizinprodukten wurde festgestellt, dass die Probleme weniger bei der Durchführung von Richtlinien für den Hersteller, sondern eher auf der Ebene der Anwender existieren. Diese werden besonders deutlich bei Betrachtung der Zielgruppe der Anwendungen, nämlich ältere oder kranke Menschen. Diese sind oft nicht in der Lage zu verstehen, wie das System funktioniert, müssen oder wollen aber auch von den Vorteilen profitieren. Aus technischen Gründen steht dem auch nichts entgegen, da keine Sachkenntnis von den Nutzern gefordert wird. Um auch dem rechtlich geforderten Sicherheitsstandard gerecht zu werden, könnten beispielsweise spezielle Kontrollmechanismen für UC eingeführt werden. Diese sollten trotzdem Sicherheit gewährleisten, jedoch dies vornehmlich durch automatisierte Kontrolle, statt einen so hohen Grad an manuellem Eingreifen zu fordern wie bisher das MPG und MPBetreibV. Durch Technikfortschritt ist es heute, ca. 15 Jahre nach Einführung des MPG viel eher möglich, Sicherheit für Patienten und Dritte eben auch auf diese Weise zu garantieren. Dazu wäre auch eine Anpassung der MPBetreibV, die solche speziellen Überprüfungsmöglichkeiten für UC zulässt, wichtig.

Anmerkung

Die Autoren sind Mitglieder im Projekt VENUS. VENUS ist ein Forschungsprojekt des interdisziplinären Forschungszentrums für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Wir danken dem hessischen Ministerium für Wissenschaft und Kunst für die Finanzierung des Projekts im Rahmen der Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE). Weiterführende Informationen erhalten Sie unter: http://www.uni-kassel.de/einrichtungen/iteg/venus/.

Interessenkonflikte

Die Autoren erklären, dass sie keine Interessenkonflikte in Zusammenhang mit diesem Artikel haben.

Literatur

1. Mattern F. Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In: Alexander R, Sommerlatte T, Winand U, Hrsg. Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlin: Springer Verlag; 2008. S. 3-29.
2. Kunze C. Ubiquitous Healthcare: Anwendung ubiquitärer Informationstechnologien im Telemonitoring [Diss, Dipl.-Ing]. Saarbrücken: Universität des Saarlandes; 2005.
3. Mattern F. Ubiquitous Computing: Szenarien einer informatisierten Welt. In: Zerdick A, et al., Hrsg. E-Merging Media – Kommunikation und Medienwirtschaft der Zukunft. Berlin: Springer Verlag; 2004.

4. Hornung G. Die digitale Identität, Rechtsprobleme von Chipkartenausweisen digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. Baden-Baden: Nomos Verlagsgesellschaft; 2005.
5. Bundesverfassungsgericht. BVerfGE 65, 1 – Volkszählung.
6. Dietz O. Datenschutz und ärztliche Schweigepflicht bei der Übermittlung von Patientendaten. Pflege- & Krankenhausrecht. 1998:98-100.
7. Gola P, Schomerus R. Bundesdatenschutzgesetz (BDSG), Kommentar. 9. Auflage. München: Verlag C.H. Beck; 2007.
8. Dierks C, Nitz G, Grau U. Gesundheitstelematik und Recht. Frankfurter Schriften Band 2. Frankfurt am Main: MedizinRecht.de Verlag; 2003.
9. Berg W. Telemedizin und Datenschutz. MedR. 2004;22(8):411-414. DOI: 10.1007/s00350-004-1225-3
10. Almer S. Das Fernbehandlungsverbot als rechtliche Grenze im Einsatz neuer Medien in der psychosozialen Versorgung. In: E-Mental-Health – Neue Medien in der psychosozialen Versorgung. Berlin: Springer Verlag; 2008. S. 13-17.
11. Dierks C. Gesundheits-Telematik – Rechtliche Antworten. DuD Datenschutz und Datensicherheit. 2006;3:142-147.
12. Quaas M, Zuck R. Medizinrecht. 2. Aufl. München: Verlag C.H. Beck; 2004.
13. Mangold H, Klein F, Stark C, Hrsg. GG-Kommentar, Bonner Grundgesetz Band 1. München: Verlag Franz Vahlen; 1999.
14. Roßnagel R. Das Recht auf (tele-)kommunikative Selbstbestimmung. Kritische Justiz. 1990;23(3):267.
15. Roßnagel A. Handbuch Datenschutzrecht. München: Verlag C.H. Beck; 2003.
16. Simitis S, Hrsg. Bundesdatenschutzgesetz – Kommentar. 6. Auflage. Baden-Baden: Nomos Verlagsgesellschaft; 2003.
17. Roßnagel A. Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. Multimedia und Recht. 2005;8(2):71-75.
18. Roßnagel A, Müller J. Ubiquitous Computing – neue Herausforderungen für den Datenschutz. Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze. Computer und Recht. 2004;20(8):625-632.
19. Roßnagel A. Datenschutz in einem informatisierten Alltag. Berlin: Friedrich-Ebert-Stiftung; 2007.
20. Höfler K. SGB V § 12 Wirtschaftlichkeitsgebot. In: Leitherer S, Hrsg. Kasseler Kommentar, Sozialversicherungsrecht. München: Verlag C.H. Beck; 2009.
21. Bizer J, Spiekermann S, Günther O. TAUCIS - Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung. Berlin: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin; 2006. Available from: https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf
22. Bake C, Blobel A, Münch P. Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen. Teil I: Datenschutz. 3. Aufl. Heidelberg, München, Landsberg, Frechen, Hamburg: Verlagsgruppe Hüthig Jehle Rehm; 2009.
23. Wollersheim U. § 5 Das ärztliche Berufsrecht. In: Terbille M, Hrsg. Münchener Anwaltshandbuch Medizinrecht. München: Verlag C.H. Beck; 2009. Rn 120-142.
24. Lenckner P. § 203. In: Schönke A, Schröder H. Strafgesetzbuch – Kommentar. 27. Auflage. München: Verlag C.H. Beck; 2006.
25. Auernhammer H. Zum Honorareinzug durch ärztliche Verrechnungsstellen. DuD Datenschutz und Datensicherheit. 1992:182.
26. Körner-Dammann M. Weitergabe von Patientendaten an ärztliche Verrechnungsstellen. Neue juristische Wochenschrift. 1992;45:729.
27. Roßnagel A, Fischer-Dieskau S. Automatisiert erzeugte elektronische Signaturen. Multimedia und Recht. 2004;3:133 - 139. Available from: http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/AR_SFD_MMR_autoSig.pdf
28. Deutsch E, Lippert HD, Ratzel R. Medizinproduktegesetz – Kommentar. Köln: Carl Heymanns Verlag; 2002.
29. Anhalt E, Dieners P. Handbuch des Medizinprodukterechts - Grundlagen und Praxis. München: Verlag C.H. Beck; 2003.
30. Kiesecker R, Kamps H. Medizinprodukte, Qualitätssicherung im Labor und eichpflichtige Gegenstände in der Arztpraxis. MedR. 2009;27(7):396-404. DOI: 10.1007/s00350-009-2439-1
31. Kirchberg D. Medizinproduktegesetz – Was Pflegende wissen müssen. Hannover: Schlütersche Verlag; 2003.

Korrespondenzadresse:
Julia Zirfas
Universität Kassel, Fachbereich Wirtschaftswissenschaften, Projektgruppe Verfassungsverträgliche Technikgestaltung, Wilhelmshöher Allee 64-66, 34109 Kassel, Deutschland
j.zirfas@uni-kassel.de

Bitte zitieren als
Skistims H, Zirfas J. Datenschutz- und Medizinprodukterecht bei Ubiquitous Computing-Anwendungen im Gesundheitssektor. GMS Med Inform Biom Epidemiol. 2011;7(2):Doc07.
DOI: 10.3205/mibe000121, URN: urn:nbn:de:0183-mibe0001216

Artikel online frei zugänglich unter
http://www.egms.de/en/journals/mibe/2011-7/mibe000121.shtml

Veröffentlicht: *04.07.2011*