vbw

Die bayerische Wirtschaft




Studie

Rechtliche Aspekte der Digitalisierung im Gesundheitswesen

Eine vbw Studie, erstellt von Prof. Dr. Dirk Heckmann

Stand: August 2017

Vorwort

Rechtsrahmen für ein digitales Gesundheitswesen weiterentwickeln

---

Die Digitalisierung erfasst seit Jahrzehnten mehr und mehr Lebensbereiche. Die Veränderungen sind enorm: Der Bogen spannt sich von der Schaffung neuer Technologien und Anwendungsgebiete bis hin zur Umgestaltung ganzer Geschäftsmodelle und Wertschöpfungsketten. Die rasante Geschwindigkeit dieses Wandels erfordert von den Akteuren einen wachsamen Blick auf Veränderungsprozesse. Unternehmen müssen schnell auf neue Bedarfe reagieren, der Gesetzgeber muss Rechtssicherheit für neue Abläufe herstellen, ohne dabei die Möglichkeiten für mehr Effizienz und Freiheit allzu sehr einzuschränken, und die Sozialversicherungen müssen sich auf völlig neue Prozesse und besser informierte, mündigere Patienten einstellen.

Gerade im Gesundheitswesen ist der digitale Transformationsprozess außerordentlich komplex und umfasst mobile Anwendungen ebenso wie telemedizinische Einsätze oder Big Data-Technologien, die nicht nur für die Forschung gänzlich neue Möglichkeiten bieten. In allen diesen Bereichen ist der Datenschutz ein nicht zu vernachlässigender Punkt. Darüber hinaus ist der geltende Rechtsrahmen nach wie vor stark vom nicht-digitalen Zeitalter geprägt, auch wenn der Gesetzgeber jüngst mit dem E-Health-Gesetz versucht hat, ihn für digitale Techniken weiter zu öffnen.

Mit unserer vorliegenden Studie *Rechtliche Aspekte der Digitalisierung im Gesundheitswesen* geben wir einen Überblick über die geltende Rechtslage und wollen damit einen Beitrag leisten, die Digitalisierung im Gesundheitswesen weiter zu fördern. Dies ist wichtig, weil die Digitalisierung wie oben beschrieben auch im Gesundheitswesen fast alle Prozesse ändern wird. Die Studie wurde erstellt von Prof. Dr. Dirk Heckmann vom Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau.

Bertram Brossardt
30. August 2017

Inhalt

1 Einleitung

Digitalisierung im Gesundheitswesen – Der Status quo

Die allgegenwärtige Digitalisierung ergreift auch und gerade das Gesundheitswesen. Von den zahlreichen in jüngerer Zeit aufgekommenen Trends sollen an dieser Stelle zwei beispielhaft aufgegriffen werden: Dies betrifft zum einen die umfassende Vernetzung aller Akteure im Gesundheitswesen, wofür in Deutschland die Telematikinfrastruktur steht. Und es ist zum anderen die Einbeziehung des Patienten selbst, der gleichsam einen Schlüssel für dieses Gesundheitsnetz erhält: Das ist die elektronische Gesundheitskarte. Beides bedarf einer gewissen Regulierung, um das entstehende System sicher und rechtskonform zu gestalten. Dies geschieht in einem eigenen E-Health-Gesetz, das viele Antworten liefert, aber auch Fragen offenlässt oder neu aufwirft.

So umstritten von Beginn an bestimmte Details einer digitalen Gesundheitsverwaltung sind: Der generelle Nutzen elektronischer Geschäftsprozesse sollte auch hier außer Frage stehen. Letztlich ist es mit E-Health ebenso wie mit E-Government, E-Business, Smart Metering oder Smart Traffic: Kommunikation und Steuerung werden schneller, zielgenauer und letztlich kostensparend, wenn sie intelligent gestaltet sind, den Akteuren einen unmittelbar einsichtigen Nutzen bringen und gegenüber Angriffen und Manipulation ausreichend abgesichert werden.

Auch im Gesundheitswesen kommt es entscheidend darauf an, dass genau jene Informationen, die ein Akteur (sei es ein Arzt, ein Apotheker oder auch ein Verwaltungsmitarbeiter) zur Aufgabenerfüllung braucht, rechtzeitig, vollständig und korrekt zur Verfügung stehen. Es ist dieser Teil eines elektronischen Gesundheitswesens, der durch das E-Health-Gesetz eine Rechtsgrundlage erhalten hat und Fortschritt anstrebt: Die Digitalisierung mit den passenden Tools und Medien sorgt für eine hohe Übertragungsgeschwindigkeit, eine standardisierte Verarbeitung und erspart Redundanzen, wie man sie zum Beispiel von der herkömmlichen Patientenaufnahme kennt. Wenn dort etwa die Empfangsstelle, das Help Desk auf der Station, die Stationsschwester, der Assistenzarzt und die Fachärztin jeweils die gleichen Fragen stellen, sieht man, dass diese Akteure zwar in standardisierter Form geschult, jedoch in keiner Weise vernetzt sind. Dabei betrifft dieser kleine Fall lediglich das Stammdatenmanagement und ganz wenige Falldaten. Wir sind noch weit entfernt von einer flächendeckenden medienbruchfreien elektronischen Aktenführung mit mobilem Datenzugriff und ausgeklügeltem Rollen-/Rechtemanagement.

Wie so etwas aussehen könnte, hat der Software-Anbieter Intersystems mit seiner Plattform „HealthShare Personal Community“ auf der Konferenz der Healthcare Information and Managements System Society in Chicago vorgestellt. Wie die Zeitung eGovernment Computing berichtete, aggregiert die Software „Daten aus allen relevanten Quellen in Echtzeit und erstellt auf Knopfdruck aktuelle, komplette Patientenakten. Über ein Portal können dann Patienten und autorisierte Angehörige die persönlichen Daten einsehen. Die Plattform soll zudem Funktionen wie die Vereinbarung von Arztterminen, die Beschaffung rezeptpflichtiger Medikamente, die Kommunikation zwischen Patient und Gesundheitsdienstleister oder auch die medizinische Aufklärung für Patienten unterstützen. Dabei soll die intuitive Nutzeroberfläche die Anwendung sehr einfach machen.“ Eingesetzt wird dieses System bereits vom Klinikbetreiber Hunterdon Healthcare System aus New Jersey, USA. Ob ein solches System nach deutschen und europäischen rechtlichen Standards und praktischen Vorstellungen umsetzbar wäre, bliebe zu diskutieren. Allemal bietet diese Diskussion interessante Orientierungspunkte für eine E-Health-Strategie.

Besonders die Ärzteschaft steht den telemedizinischen Verfahren mit Skepsis gegenüber. Manche befürchten, die Ärzte könnten durch deren Einführung nach einer gewissen Zeit ihre Patienten und damit ihre berufliche Lebensgrundlage verlieren. Andere wiederum sehen den persönlichen Arzt-Patienten-Kontakt als eine derart wichtige Voraussetzung an, dass es nicht hinnehmbar wäre, müsste sich der Arzt nur auf Angaben des Patienten oder auf übermittelte Patientendaten verlassen, ohne sich selbst einen persönlichen Eindruck verschaffen zu können.

In der Tat scheint Deutschland im Vergleich zu anderen Ländern weit zurück zu liegen: „Papierlose Klinik bleibt Vision“ titelte Price Waterhouse Coopers. Die EU-Studie „Benchmarking Deployment of E-Health-Services 2012-2013“ kritisierte gar unzureichende Datensicherheit: So sei die Verschlüsselung der gespeicherten Patientendaten nur in 40 Prozent der deutschen Kliniken üblich. 75 Prozent sicherten ihre IT nur mit einem Passwort. Nur 20 Prozent hätten ein redundantes Datensicherungssystem. Und in 33 Prozent der deutschen Kliniken erfolge eine Datenherstellung nach Systemausfall erst nach 24 Stunden.

So groß der Nutzen innovativer digitaler Technologien, Prozesse und Strukturen auch ist: Man wird allem skeptisch gegenüberstehen, wenn und soweit die IT-Sicherheit nicht gewährleistet ist. Und noch mehr: Gerade im Gesundheitswesen ist Sicherheit eine zentrale Herausforderung. Das betrifft sowohl das individuelle Vertrauensverhältnis des Patienten zum Arzt (z.B. in die Validität der Befunde) als auch das generelle Systemvertrauen in Geschäftsabläufe wie Abrechnungen, Terminplanung etc. Um dies in dem notwendigen Maß zu gewährleisten, braucht man stabile, gesicherte Server, ein ausgeklügeltes Rollen-/Rechtemanagement, Interoperabilität der Systemkomponenten und eine sichere Datenübertragung. Dafür bedarf es erheblicher Anstrengungen, folgt man den Lageberichten des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Diese gehen von einer erheblichen und exponentiell gesteigerten Bedrohungslage aus, nicht zuletzt wegen der Professionalisierung der Cyberangriffe, für die E-Health

leider auch ein lohnendes Betätigungsfeld sein kann. Letztlich kann/muss man dem ein Höchstmaß an Professionalisierung der Telematikinfrastruktur entgegensetzen.

Am Ende kommt es auch darauf an, sinnvolle Standards für Online-Konsultationen, internetbasierte Erstdiagnosen und telemedizinische Verfahren zu erarbeiten.
So bleibt neben der Nützlichkeit und der Sicherheit die Frage nach der Rechtskonformität digitaler Gesundheitsvorsorge und Gesundheitsverwaltung. Darf im Rahmen der Digitalisierung alles getan werden, was nützlich und sicher erscheint? Wo liegen die rechtlichen Anforderungen und Grenzen? Dem widmet sich die vorliegende Studie. Sie soll (bayerischen) Unternehmen die Chancen der Digitalisierung im Gesundheitswesen näher bringen, dabei aber auch die rechtlichen Risiken in den Blick nehmen.

2 Akteure und Interessen

Ein Überblick

Wenn man die Chancen und Risiken der Digitalisierung im Gesundheitswesen betrachtet, sind es verschiedene Akteure, deren Interessen für die Gestaltung neuer Geschäftsprozesse zu berücksichtigen sind.

- Leistungsempfänger bzw. -berechtigte (Patienten/Nutzer)
- Leistungserbringer (Ärzte, Krankenhäuser, Apotheker, Heilberufe)
- Leistungsträger (Krankenkassen)
- Wirtschaftsunternehmen (Hersteller, IT-Dienstleister, Softwareentwickler etc.).

2.1 Perspektiven, Entwicklungen, Erwartungen

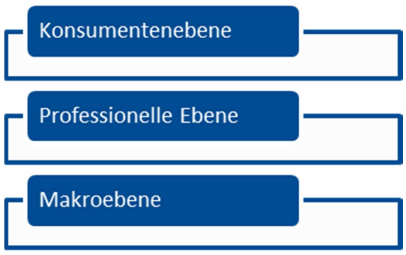
Je nachdem, welche Perspektive man einnimmt, sind unterschiedliche Erwartungshaltungen im Hinblick auf die technische Entwicklung eines digitalisierten Gesundheitswesens zu verzeichnen.

2.1.1 Perspektiven

So unterscheidet das Beratungsunternehmen Deloitte drei Ebenen der Digitalisierung im Gesundheitswesen.[1]

[1] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 4, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

Abbildung 1
Digitalisierungsebenen im Gesundheitswesen



Die Konsumentenebene nimmt die Perspektive des Nutzers als Konsument digitaler Gesundheitsdienstleistungen ein. Auf dem hierdurch adressierten sog. zweiten Gesundheitsmarkt werden etwa webbasierte Gesundheitsportale, Apps oder Mess- und Assistenzsysteme nachgefragt.

Demgegenüber umfasst die Professionelle Ebene die Perspektive der Leistungserbringer im Gesundheitssektor mit jenen Produkten und Dienstleistungen, die durch sie initiiert und/oder finanziert werden.

Die Makroebene beschreibt schließlich die Vernetzung der einzelnen Angebote, um einen effizienten und sicheren Informationsaustausch zwischen allen beteiligten Akteuren zu ermöglichen.

Insgesamt soll die Digitalisierung auf allen Ebenen zu einer besseren und flächendeckenden Versorgung, einer höheren Qualität der Behandlung und einer transparenteren und effektiveren Dokumentation führen.[2]

2.1.2 Entwicklungen

Die technische Entwicklung im Gesundheitswesen schreitet auf der Ebene der Konsumenten rasant voran. Seit 2009 steigt die Zahl der Smartphone-Besitzer stetig, von 6 Millionen auf ca. 49 Millionen (Stand April 2016).[3] Nach Schätzungen von Deloitte verwendeten Ende 2014 knapp die Hälfte aller deutschen Smartphone-Nutzer ihre privaten Endgeräte für digitale Gesundheitsangebote.[4] Gründe für diese Entwicklung sind

[2] http://www.aekno.de/page.asp?pageID=14590 (zuletzt abgerufen am 01.08.2017).
[3] http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/ (zuletzt abgerufen am 01.08.2017).
[4] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 4, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017).

ein steigendes Gesundheitsbewusstsein bei der Bevölkerung, der allgemeine Digitalisierungsfortschritt, die Allverfügbarkeit von Netzen, die laut Bitkom bei 90 Prozent der Haushalte mit einer Bandbreite von über 6 Mbit/s vorhanden ist[5], und die Etablierung von Endgeräten wie Smartphones und Tablets.[6]

In den anderen beiden Ebenen gestaltet sich dieser Fortschritt etwas langsamer. Dies ist etwa mit Blick auf die Professionelle Ebene dem Umstand geschuldet, dass die traditionellen Leistungserbringer der Digitalisierung im Gesundheitswesen jahrelang überwiegend skeptisch und ablehnend gegenüber standen.[7] Der „neumodische Trend" entsprach dabei nicht ihrem Vorstellungsbild von einer für sie typischen Arzt-Patienten-Beziehung. In der Folge haben sich andere OECD-Staaten – wie z.B. Österreich – im E-Health-Sektor schon derart weiterentwickelt, dass Deutschland im Vergleich hierzu hinterher hinkt. Die E-Health-Studie „Ärzte im Zukunftsmarkt 2015" zeigt aber, dass die Berührungsängste bezüglich der Digitalisierung zunehmend abgelegt werden. Zwei Drittel der Ärzte stehen neuen Kommunikationsformen wie Videokonsilen mit Kollegen oder der Videokommunikation mit Pflegediensten offen gegenüber. Ein Drittel kann sich auch vorstellen, auf diese Weise mit Patienten zu kommunizieren. Erst wenn sich alle Beteiligten zum Fortschritt durch Digitalisierung bekennen, können professionelle digitale Dienste im Gesundheitswesen flächendeckend etabliert werden.

Auf der Makroebene zeigt sich am Beispiel der elektronischen Gesundheitskarte, wie die Entwicklung durch rechtliche und technische Hürden derzeit an einigen Stellen stagniert. Grundsätzlich wurde zwar in § 291a SGB V der rechtliche Rahmen für die Umsetzung und vollumfassende Einführung der elektronischen Gesundheitskarte geschaffen. So gibt etwa § 291a Abs. 3 SGB V vor, welche Anwendungen die Gesundheitskarte unterstützen muss und wie die Datenverarbeitung und -nutzung technisch auszugestalten ist. Zudem finden sich in dieser Vorschrift noch weitere datenschutzrechtliche Vorgaben, bei denen auch erkennbar wird, dass oberste Handlungsmaxime die Gewährleistung informationeller Selbstbestimmung des Patienten ist. Eine vollständige und lückenlose Umsetzung dieser Vorgaben konnte aber bis heute nicht realisiert werden.[8] Konkret stellt sich etwa die Frage, wo die personenbezogenen Daten gespeichert werden sollen. Grundsätzliche Möglichkeiten sind eine zentrale Speicherung, eine Speicherung auf der Gesundheitskarte, eine externe Speicherung auf einem USB-Stick oder eine kombinierte Speicherung. Für jede dieser Alternativen ergeben sich rechtliche wie technische Worstcase-Szenarien, vom Hacker-Angriff über individuellen

---

[5] Bitkom Presseinfo „Breitband Europa", 21.01.2014, http://www.bitkom-research.de/Presse/Pressearchiv-2014/Breitbandausbau-Deutschland-in-der-Spitzengruppe (zuletzt abgerufen am 01.08.2017).
[6] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 6, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017).
[7] Bitkom, e-Health Blog: Ärzte öffnen sich digitalen Innovationen, https://www.bitkom.org/Presse/Blog/eHealth-Studie-Aerzte-oeffnen-sich-digitalen-Innovationen.html (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[8] Buchner, MedR 2016, 660, 662 f. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

Datenverlust bis hin zu gestohlenen Praxiscomputern. Solange für diese ganz zentrale Frage keine allgemein akzeptierte Lösung gefunden wird, werden noch viele neue Funktionen der elektronischen Gesundheitskarte auch in Zukunft keine flächendeckende Verbreitung finden. Gerade in Bezug auf Datensicherheit wird das System den Ansprüchen noch nicht vollständig gerecht und scheint auch nicht ausgereift zu sein.

2.1.3 Erwartungen

Sowohl der Patient als Leistungsempfänger als auch die traditionellen Leistungserbringer und die Wirtschaftsunternehmen haben Erwartungen an die Digitalisierung im Gesundheitswesen. Für den Patienten hat eine gute Kommunikation mit dem zu behandelnden Arzt oberste Priorität. Er schätzt das vertrauliche Gespräch ebenso wie die Gewissheit, dass ihm zugehört wird. So stellt es für ihn kein Problem dar, dass die Digitalisierung eine immer größere Rolle in der medizinischen Betreuung spielt, solange die Kommunikation dadurch nicht erschwert oder gar verhindert wird. Im Rahmen einer Umfrage im Jahr 2015 zeigte sich, dass 58 Prozent der Befragten die Verwendung von IT im Untersuchungsraum als positive Erfahrung verzeichnen und sie die Technologie als wertsteigernden Faktor ihrer Behandlung empfinden.[9]
Viele Patienten versuchen mittlerweile auch darüber hinaus, den Wert der ärztlichen Konsultation dahingehend zu maximieren, dass sie sich vor dem Arztgespräch online informieren oder auch indem sie Daten von externen Geräten zur Gesprächsgrundlage mit dem Arzt machen.

Neben den Patienten haben auch die traditionellen Leistungserbringer diverse Erwartungen. So befürchten beispielsweise Ärzte durch die Digitalisierung einen erheblichen Mehraufwand. Aus ihrer Sicht könnte sich ein solcher bei der elektronischen Gesundheitskarte etwa dadurch ergeben, dass sie quartalsmäßig die Versichertenstammdaten gem. § 291 Abs. 2b Satz 3 SGB V aktualisieren und den dort vorgesehenen Notfalldatensatz erstellen müssen.[10] Die Ärzte sind überdies teilweise der Auffassung, dass sie die Einführung der elektronischen Patientenakte Zeit kostet, die sie für das Vier-Augen-Gespräch mit dem Patienten benötigen. Die Einführung eines elektronischen Medikationsplans gem. § 31a SGB V birgt ihrer Ansicht nach die Gefahr, dass auch andere im Gesundheitswesen Tätige, wie etwa Apotheker, diesen abändern könnten und dadurch Unklarheiten hinsichtlich der Gültigkeit entstehen.[11] Um diese Ängste beseitigen zu können, muss im Zuge der Digitalisierung sichergestellt werden, dass diese weder eine Überlastung der Arztpraxen mit sich bringt noch die Qualität der medizinischen Be-

---

[9] Nuance, Die Gesundheitsversorgung aus Sicht der Patienten, S. 18, http://www.nuance.de/groups/healthcare/@web-de/documents/collateral/nc_037943.pdf (zuletzt abgerufen am 01.08.2017).
[10] Paland/Holland, NZS 2016, 247, 251, 252.
[11] http://www.finanzen.de/news/16932/e-health-aenderungen-bei-gesundheitskarte-stellt-aerzte-vor-probleme (zuletzt abgerufen am 01.08.2017).

handlung in Frage gestellt wird. Zudem sind die sich auch hieraus ergebenden möglichen Vorteile wie etwa in Gestalt von Zeitersparnissen oder einer besseren Diagnostik zu berücksichtigen.

Aus Sicht der Leistungsträger, mithin der Krankenkassen, fehlt es an einem übergreifenden Rahmen zur digitalen Vernetzung.[12] Für sie stellen sich Probleme in den Bereichen Umsetzung des Datenschutzes, geeignete Software, Höhe des Personalaufwandes und zu erwartende Kosten. Die Krankenkassen versprechen sich aber durch die Digitalisierung Effizienzgewinne, die sich langfristig durch eine Prozesskostensenkung bemerkbar machen sollen. Für eine solide Ausgangslage sehen sie den Startpunkt in der Umgestaltung ihrer Prozesse.

Zu berücksichtigen sind schließlich auch die Erwartungen der Unternehmen, die als Hersteller, IT-Dienstleister etc. an der Digitalisierung beteiligt sind. Die Vermarktung eines sogenannten „Medizinproduktes“ bedarf der Zertifizierung durch das Bundesinstitut für Arzneimittel und Medizinprodukte, dessen Verfahren meist schwierig und nicht immer bekannt ist, weswegen aus Sicht der Unternehmen ein Leitfaden zur Vereinfachung der Digitalisierung in der Unternehmensbranche wünschenswert wäre. Zudem bestehen bei den etablierten Unternehmen Befürchtungen dahingehend, dass sie im Zuge der Digitalisierung von neuen Marktteilnehmern verdrängt werden.[13] Über kurz oder lang bewirke die Digitalisierung nämlich eine Neuordnung der Rollen, weshalb für fortbestehende Erfolge eines Unternehmens die strategische Kooperation immer wichtiger werde. Überdies können sich für zahlreiche Unternehmen auch erhebliche Potenziale und Chancen durch die Digitalisierung ergeben, angefangen von der Vereinfachung und Effektivierung bestimmter Verfahrensabläufe bis hin zur Erschließung völlig neuer Geschäftsmodelle.

2.2 b2c (Konsumentenebene): Der Patient als Nutzer und Co-Leistungserbringer

Im sogenannten zweiten Gesundheitsmarkt ist der Patient als Nutzer und Co-Leistungserbringer der Hauptakteur in der Konsumentenebene, sowohl hinsichtlich der Nutzung von Gesundheitsportalen und Apps als auch von Mess- und Assistenzsystemen.

---

[12] http://www.versicherungsbote.de/id/4820197/PKV-GKV-Digitalisierung-Datenschutz-Prozesse/ (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[13] https://www.rolandberger.com/de/press/Press-Release-Details_6720.html (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

2.2.1 Gesundheitsportale

Gesundheitsportale sind seit vielen Jahren fester Bestandteil im Consumer E-Health-Angebotskatalog. Endverbraucher möchten sich über Gesundheitsthemen informieren und mit anderen austauschen. So finden sowohl Frage-Antwort-Foren (sogenannte Patienten-Plattformen), auf denen medizinisches Fachpersonal fehlt, als auch Patienten-Mediziner-Plattformen, in die Ärzte und Medizinjournalisten eingebunden sind, großen Zuspruch.[14] Schwierig gestaltet sich bei den Patienten-Plattformen allerdings die Sicherstellung der Qualität der Antworten. Die Patienten-Mediziner-Plattformen hingegen liefern dem Nutzer schnell und unkompliziert Input, der zwar selten falsch, dafür aber lückenhaft sein kann. Jeder dritte Deutsche informierte sich laut Stiftung Warentest schon 2009 mindestens einmal pro Monat über solch ein Portal.[15] Alleine der Anbieter netdoktor.de verzeichnete im Jahr 2009 45.000 Besucher am Tag. 2015 ergab sich in Bezug auf dieses Portal bereits eine Netto-Reichweite von 2,36 Millionen Besuchern pro Monat.[16]

2.2.2 Apps

Zunehmende Bedeutung in einem digitalisierten Gesundheitswesen erhalten Apps und smarte Fitness-Tools. Der weltweite Markt soll Schätzungen zufolge für mobile E-Health-Angebote bis zum Jahr 2017 ein Umsatzvolumen von 26 Milliarden Dollar erreichen, an dem Europa mit 6,9 Milliarden Dollar beteiligt sein wird.[17] Damit eignet sich gerade dieser Bereich für junge und innovative Start-up-Geschäftsideen. Ausgerichtet auf die Nutzerbedürfnisse entwickeln sich immer mehr Angebote in den Bereichen Organisation, Behandlung, Prävention und Information.

So hat das Münchner Start-up „MyTherapy“ eine sogenannte Kalender-App entwickelt, die Auskunft über die Einhaltung der Therapieziele gibt und damit ein persönliches

---

[14] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 8, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017).

[15] Stiftung Warentest, Gesundheitsportale: Die besten Infos im Netz, 05.06.2009, https://www.test.de/Gesundheitsportale-Die-besten-Infos-im-Netz-1780855-0/ (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

[16] https://www.agof.de/download/Downloads_Internet_Facts/Downloads_Internet_Facts_2015/Downloads_Internet_Facts_2015-03/03-2015_Berichtsband%20zur%20internet%20facts%202015-03.pdf?x87612 (zuletzt abgerufen am 01.08.2017).

[17] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 9, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

Gesundheitstagebuch bereithält.[18] Das Hamburger Start-up Sonormed hat mit „Tinnitracks“ eine Behandlungs-App entwickelt, die es Tinnitus-Betroffenen ermöglicht, Musikstücke anzuhören, aus denen Tinnitus-Frequenzen herausgefiltert werden, was dazu führt, dass die überaktiven Nervenzellen im Hörzentrum gehemmt werden. Das Dresdner Start-up „Caterna Vision“ hat eine Sehschule für Kinder entwickelt, die eine Behandlung von durch einseitiges Schielen auftretender Schwachsichtigkeit zu Hause ermöglicht. Im Bereich der Diät-Apps haben sich „Weight Watchers“ und viele andere mit Ernährungsplänen, Rezeptvorschlägen und Kalorienzählern am Markt platziert. In einer Umfrage aus dem Jahre 2015 zeichnete sich das anhaltende Bewusstsein innerhalb der Bevölkerung für ein „gesünderes Leben“ bereits ab.[19] Von den über 5.000 Befragten gaben 32 Prozent, die mit ihrem Partner zusammen in einem Haushalt leben, an, Digital Health Applikationen wie Rezepte zur gesunden Ernährung zu nutzen. Angelehnt an das Start-up-Modell aus Köln, das ein Portal namens „BetterDoc“ entwickelt hat, mit dem der passende Facharzt für die jeweiligen Beschwerden des Nutzers gefunden werden kann[20], wurden auch sogenannte Verzeichnis-Apps entwickelt, die die Suche nach Ärzten, Krankenhäusern etc. erleichtern sollen. Teilweise gewähren sie dabei auch Zugriff auf Bewertungen und Empfehlungen anderer Patienten. Immer größerer Beliebtheit erfreuen sich aber allen voran smarte Fitness-Apps. Nach einer Presseinformation von Bitkom verwendeten 2013 bereits 57 Prozent der deutschen Hobbysportler ihr Smartphone in Kombination mit einer solchen App[21], wie z.B. „Runtastic“. Der Grund für die zunehmende Nutzung solcher Apps liegt in ihrer Multifunktionalität. So beschränkt sich deren Funktion nicht nur auf Pulsmessung oder Schrittzählung, vielmehr kann die über die gelaufene Strecke, gefahrene Zeit oder verbrauchten Kalorien durchgeführte Leistungsmessung archiviert, analysiert und gerade auch in sozialen Netzwerken geteilt und kommentiert werden. Damit wird eine Brücke zwischen dem Unterhaltungsfaktor und der Gesundheitsanwendung geschlagen. Nicht zuletzt können die ermittelten Trainings- und Vitaldaten an einen Sportmediziner übertragen werden, was überdies die Diagnose- und Behandlungsqualität positiv beeinflussen kann.[22]

---

[18] E-Health Blog, 10 deutsche eHealth Start-ups, die überzeugen, 06.06.2016, https://ehealthblog.de/2016/06/06/10-deutsche-ehealth-start-ups-die-ueberzeugen/ (zuletzt abgerufen am 01.08.2017).

[19] https://de.statista.com/statistik/daten/studie/454442/umfrage/nutzer-von-digital-health-applikationen-und-services-nach-partner-im-haushalt/ (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

[20] E-Health Blog, 10 deutsche eHealth Start-ups, die überzeugen, 06.06.2016, https://ehealthblog.de/2016/06/06/10-deutsche-ehealth-start-ups-die-ueberzeugen/ (zuletzt abgerufen am 01.08.2017).

[21] Bitkom Presseinfo „Hobbysportler nutzen neue Technologien“, 29.11.2013, http://www.bitkom-research.de/Presse/Pressearchiv-2013/Hobbysportler-nutzen-neue-Technologien (zuletzt abgerufen am 01.08.2017).

[22] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 12, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017).

2.2.3 Mess- und Assistenzsysteme: Wearables

Im Kontext der Digitalisierung darf auch der Markt der sogenannten Wearables nicht unberücksichtigt bleiben. Dieser Markt besteht aus Computertechnologien, die am Körper oder auf dem Kopf getragen werden. Bekannt sind Smartwatches, Fitnessarmbänder, Brillen und Brustgurte. Sie dienen als Applikator in den Bereichen Bewegung, Ernährung und Schlaf. Am Beispiel einer Smartwatch, die am Handgelenk getragen wird, kann die Anzahl der Schritte im Alltag erfasst und häufig auch zur Schlafmessung eingesetzt werden. Sie motiviert so zu einem aktiveren Alltag und mehr Schlaf. Genutzt wird dafür eine günstige und technisch einfach realisierbare Beschleunigungsmessung.[23] Andere Lösungen hingegen verfügen zusätzlich über einen optischen Pulssensor, der es ermöglicht, ohne Brustgurt Messungen vorzunehmen. Anschließend wird das gewonnene Wissen verwendet, um Herzfrequenz und Energieverbrauch des Nutzers genauer berechnen und dadurch bessere Gesundheitsempfehlungen geben zu können. Zukünftig dürfte das Verfahren des optischen Pulssensors für viele Wearables zum Standardrepertoire gehören. Aber nicht nur im präventiven Bereich etablieren sich Mess- und Assistenzsysteme, sie ersetzen inzwischen auch die klassischen krankheitsbegleitenden Messgeräte.[24] In diese Kategorie sind etwa Alarmfunktionen einzuordnen, die sich aktivieren, sobald eine Messung den vorgegebenen Wertebereich verlässt und dies elektronisch an den behandelnden Arzt weiterleiten.

2.3 b2b (Professionelle Ebene): IT-Dienstleistungen und Technik für Gesundheitsberufe

Innerhalb des sogenannten ersten Gesundheitsmarktes sind die traditionellen Leistungserbringer Hauptakteure in der Professionellen Ebene.[25] Zu den traditionellen Akteuren zählen beispielsweise Ärzte, Krankenhäuser und Pflegedienste. Sie initiieren und/oder finanzieren digitale Gesundheitsangebote wie spezifische Online-Plattformen für Ärzte, die Telemedizin, mHealth und Ambient Assisted Living (AAL). Auch wenn der Versicherungsnehmer bzw. Patient am Ende Nutznießer solcher Innovationen sein mag, geht es bei dieser Perspektive um deren professionelle Bereitstellung.

---

[23] Schuhmacher, in: Andelfinger/Hänisch, eHealth, 2016, S. 41 f. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[24] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 12, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[25] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 4, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 01.08.2017).

2.3.1 Spezifische Online-Plattformen für Ärzte

Spezifische Onlineportale wie z.B. „DMPsysOnline“[26], „medi“[27] und „Smart Radiology“[28] erleichtern den Arbeitsalltag von Ärzten in vielerlei Hinsicht. „DMPsysOnline“ unterstützt etwa den Arzt bei der Datenerfassung von Disease-Management-Programm (DMP)-Dokumentationen, indem über chronisch kranke Patienten ein Patientenstamm angelegt wird, der direkt an die Datenstelle des DMP-Systems übermittelt wird.[29] Zusätzlich erinnert dieses System den Arzt über eine Reminder-Funktion an die laufenden, im Quartal noch auszustellenden Dokumente. Das Ärzteportal „medi“ bietet durch die Bereitstellung von Arbeitshilfen wie etwa Rezeptbeispielen und Broschüren sowie durch die Aufbereitung interessanter Studien ebenfalls Erleichterung im Ärztealltag.[30] Die Plattform „Smart Radiology“ vereinfacht dem Arzt das Erstellen der radiologischen Befunde, indem sie ihm – anhand der untersuchungsspezifischen Checkliste im Portal – die aus medizinischer Sicht zu bewertenden Aspekte in einem Entscheidungsbaum darstellt.[31] Hieran kann er simultan einen linguistisch korrekten Befundtext erstellen, der die Vergleichbarkeit und Reproduzierbarkeit von Befunden verbessert, die Qualität sichert und die Effizienz durch Zeitersparnis beim Tippen steigert. Von den in Deutschland tätigen 6.800 Radiologen haben sich auf Grund dieser Vorzüge seit dem Launch im Januar 2016 bereits mehr als 1.100 Nutzer registriert. Obwohl das Portal bisher nur in deutscher Sprache veröffentlicht ist, wird es in über 34 Ländern verwendet. Die Idee des Smart Reporting ist aus dem ärztlichen Alltag heraus von Ärzten für Ärzte entstanden; es soll in nächster Zeit auch auf den Sektor der Traumatologie erweitert werden.

2.3.2 Telemedizin

Die Telemedizin beschreibt einen Teilbereich der Telematik im Gesundheitswesen.[32] Sie bildet die Verbindung zwischen Telekommunikation und Informatik. Medizinische Daten werden dabei nicht nur gespeichert, sondern auch über Datennetze übermittelt. Ziel ist es, die Daten eines Patienten verfügbar zu machen, um die sektorübergreifende medizinische Versorgung zu verbessern. Darüber hinaus können medizinische Leistungen trotz räumlicher Distanz ermöglicht werden, was zur Folge hätte, dass der weit verbreitete Ärztemangel in ländlichen Regionen aufgefangen werden kann. Die Telemedizin wird in die Telekonsultation und das Telemonitoring unterteilt.

---

[26] http://www.dmpservices.de/index.php/aerzte-kliniken/arztonlineportal (zuletzt abgerufen am 01.08.2017).
[27] https://www.medi.de/arzt/ (zuletzt abgerufen am 01.08.2017).
[28] eGovernment Computing, Interview mit Prof. Dr. med. Wieland und Andreas Klüter, eHealth Portal für Radiologen, Nr. 12/2016, S. 11.
[29] http://www.dmpservices.de/index.php/aerzte-kliniken/arztonlineportal (zuletzt abgerufen am 01.08.2017).
[30] https://www.medi.de/arzt/ (zuletzt abgerufen am 01.08.2017).
[31] Interview mit Prof. Dr. med. Wieland und Andreas Klüter, eHealth Portal für Radiologen, eGovernment Computing Nr. 12/2016, S. 11. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[32] Schmid, in: Andelfinger/Hänisch, eHealth, 2016, S. 12. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

2.3.2.1 Telekonsultation

Die Telekonsultation beschreibt die Fernkommunikation zwischen den Ärzten.[33] Ein behandelnder Arzt kann sich durch moderne Telematik von nicht ortsansässigen Kollegen eine zweite Meinung zum vorliegenden Krankheitsbild und zum Vorgehen bei der Behandlung einholen. So können Spezialisten hinzugezogen werden, ohne dass sie vor Ort sein müssen. Eine Abwandlung hiervon ist die Telechirurgie, bei der im Rahmen von Operationen Telekommunikationstechniken und/oder Robotersysteme zum Einsatz kommen, die einen Expertenaustausch oder auch eine ferngesteuerte Operation über größere Distanzen hinweg ermöglichen.[34]

2.3.2.2 Telemonitoring

Mittels Telemonitoring können chronisch kranke Patienten durch Fernbetreuung in ihrer gewohnten Umgebung bleiben und werden trotzdem von geeigneten Ärzten betreut und beraten.[35] Einem an Diabetes mellitus Erkrankten wird beispielsweise ein Blutzuckermessgerät zur Verfügung gestellt, mit dem er seine Vitalparameter bestimmen kann. Die hierüber erfassten Daten werden sodann an die behandelnden Ärzte übermittelt. Der Patient lernt so auch schrittweise mit der Krankheit umzugehen.

Eine Ferndiagnose ohne jegliche Untersuchung des Patienten vor Ort ist demgegenüber in Deutschland nicht ohne weiteres möglich, da in der Musterberufsordnung für Ärzte (§ 7 Abs. 4) ein Fernbehandlungsverbot verankert ist. Einzig eine Aufhebung bzw. Lockerung dieses Verbotes durch den deutschen Gesetzgeber könnte solche Vorgänge legalisieren.

2.3.3 mHealth

E-Health avanciert zunehmend zu mHealth (mobile Health) und verbindet damit eine signifikante Verbesserung des mobilen Einsatzes digitaler Technologien mit dem Gedanken der Digitalisierung im Gesundheitswesen. So wird etwa das Krankenhausinformationssystem durch eine Vernetzung mit mobilen Endgeräten dadurch verbessert, dass beispielsweise das schnelle und unkomplizierte Abrufen von Patientendaten bei der Visite mittels Tablet-PCs ermöglicht wird.[36] mHealth bringt dabei nicht nur organisatorische Vorteile mit sich, sondern bietet grundsätzlich jedem einzelnen Leistungserbringer einen großen Wettbewerbsvorteil. Denn durch die Integration und die Imple-

---

[33] http://www.telemedallianz.de/witm_an_konsultation.html (zuletzt abgerufen am 01.08.2017).
[34] http://www.telemedallianz.de/witm_an_chirugie.html (zuletzt abgerufen am 01.08.2017); Schmid, in: Andelfinger/Hänisch, eHealth, 2016, S. 15.
[35] Schmid, in: Andelfinger/Hänisch, eHealth, 2016, S. 13 f. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[36] http://medizin-und-neue-medien.de/tag/mhealth/ (zuletzt abgerufen am 02.08.2017).

mentierung in ein bestehendes System können zum einen Mitarbeiter entlastet werden, zum anderen lässt sich die Effizienz durch optimierte Versorgungs- und Kommunikationsprozesse sowie auch die Patientenzufriedenheit steigern. Am Beispiel eines sogenannten „Smart Services" kann das Angebot eines Leistungserbringers durch einen mobilen Prozess erweitert werden.[37] Demgemäß hat Anfang 2016 ein Hausarzt aus der Nordpfalz ein Online-Sprechzimmer in Form einer Messenger-App namens „meinarztdirekt.de" eingerichtet.[38] Ausschlaggebend für dieses Angebot war, dass er – wie er selbst berichtet – seit 14 Jahren als hausärztlich tätiger Landarzt in einer Einzelpraxis niedergelassen ist und die teils langen Wege der Patienten zur Sprechstunde kennt. Aus dieser Überlegung heraus entwickelte er für Patienten einen Messenger, bei dem sie sich registrieren können und dadurch einen persönlichen Zugangscode erhalten, mit dem sie ihr Benutzerkonto mit dem des Arztes verknüpfen, um so mit ihm Kontakt aufnehmen zu können. Dabei werden die Nutzerdaten innerhalb des Portals und auf deutschen Servern gespeichert. Der Vorteil dieser Messenger-Konversation ist, dass der Arzt flexibel und zeitlich ungebunden antworten kann und nicht wie bei einer Videosprechstunde terminlich fixiert ist. Je nach Zeitaufwand rechnet er nach Ziffer 1 oder 3 der Gebührenordnung für Ärzte (GOÄ) ab; die Rechnung kann dann durch gängige Online-Bezahlsysteme beglichen werden. Privatpatienten können diese Rechnung bei ihrer Versicherung einreichen. Für Kassenpatienten handelt es sich bisher noch um eine Selbstzahlerleistung. Aufgrund der durchweg positiven Resonanz der Patienten auf das dargestellte mHealth-Angebot wurde dieses bereits von mehreren Ärzten aus verschiedenen Fachgruppen übernommen.

2.3.4 Ambient Assisted Living (AAL)

Im Pflegesektor sollen Ambient Assisted Living (AAL)-Systeme den digitalen Fortschritt vorantreiben. Sie bestehen aus den Komponenten E-Health- und Smart-Home-Technologien.[39] Es handelt sich dabei um Modelle, die helfen sollen, möglichst lange ohne fremde Hilfe in der gewohnten Umgebung leben zu können. Darüber hinaus sollen professionelle Pflegekräfte oder auch pflegende Angehörige sowohl zeitlich als auch körperlich entlastet werden. Als Zielgruppe werden ältere und/oder pflegebedürftige Personen fokussiert, die ansonsten stationärer Pflege bedürften. AAL stößt jedoch derzeit eher auf Ablehnung als auf Zuspruch. Dies ist zu einem nicht unbeachtlichen Teil dem Umstand geschuldet, dass sich kaum jemand von sich aus mit dem Älterwerden oder gar Gebrechen beschäftigen möchte. Hinter den AAL-Systemen steckt jedoch ein wertvoller Gedanke, den es im Zuge der Digitalisierung weiter auszubauen gilt.

---

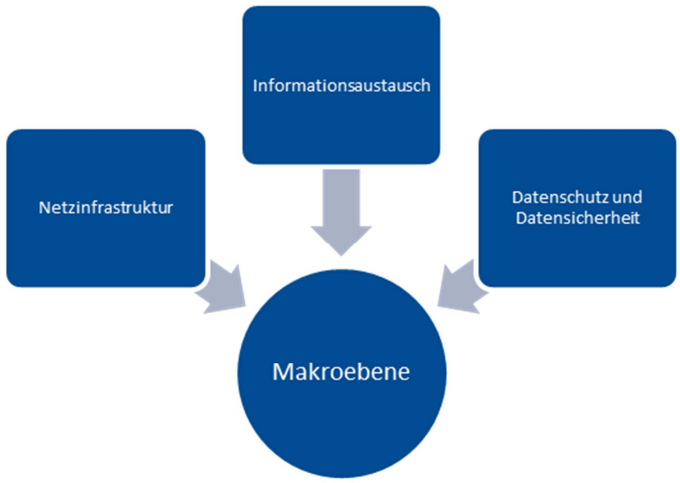
[37] https://www.smartcircles.de/ (zuletzt abgerufen am 22.11.2016).
[38] ÄrzteZeitung, WhatsApp für Ärzte, 08.11.2016, http://www.aerztezeitung.de/praxis_wirtschaft/aerztliche_verguetung/article/922994/whatsapp-aerzte.html (zuletzt abgerufen am 02.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[39] Andelfinger, in: Andelfinger/Hänisch, eHealth, 2016, S. 241 ff. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

Denn die Technologie kann ein sorgenfreieres Leben in den eigenen vier Wänden ermöglichen. Im Zeitalter von steigenden Pflegeversicherungsbeiträgen kann AAL auch für sozial schwächere Gesellschaftsschichten eine Perspektive darstellen. So sind Geschäftsmodelle wie „REMEO“, das langzeitbeatmeten Patienten eine ambulante Versorgung zu Hause ermöglicht, oder „Sicherheit im Zuhause und unterwegs“, das durch sensorgestützte Technik Stürze verhindern soll, ernst zu nehmende Optionen für eine zukunftsorientierte Gesellschaft.[40]

2.4 b2all (Makroebene): Digitale Infrastruktur im Gesundheitswesen

Die Makroebene betrifft als übergreifender Rahmen die Vernetzung der digitalen Gesundheitsangebote.[41] Dafür wird eine flächendeckende Infrastruktur benötigt, die den Informationsaustausch zwischen Patienten, Ärzten, Krankenkassen etc. ermöglicht und den Schutz und die Sicherheit der Patientendaten gewährleistet.

Abbildung 2
Digitale Infrastruktur im Gesundheitswesen



[40] http://www.dienstleistungundtechnik.de/pdfs-meta/pdfs-verbuende/ehealthathome/Tagungsmappe_nov2011_Abschlussveranstaltung%20eHealth.pdf (zuletzt abgerufen am 02.08.2017).
[41] Deloitte, Studie Perspektive E-Health – Consumer-Lösungen als Schlüssel zum Erfolg, S. 4, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/tmt-studie-perspektive-ehealth.html (zuletzt abgerufen am 02.08.2017).

2.4.1 Netzinfrastruktur

Um die Digitalisierung im Gesundheitswesen weiter voranzutreiben, bedarf es einer leistungsfähigen, flächendeckenden, digitalen Infrastruktur. Die Bewertung der digitalen Infrastruktur Bayerns fällt im bundesweiten Vergleich zwar positiv aus, jedoch besteht im internationalen Vergleich durchaus noch Aufholbedarf.[42] Es zeigt sich, dass nach wie vor Defizite im Übergang vom stationären zum ambulanten Bereich zu verzeichnen sind.[43] Die fehlende Vernetzung ist dabei besonders spürbar, da die Bereiche überwiegend in ihren IT-Infrastrukturen arbeiten, welche mit den IT-Systemen aus anderen Sektoren nicht immer kompatibel sind. Ziel der sogenannten Telematikinfrastruktur ist es daher, die sektorale IT-Gliederung zu überwinden. Das am 01.01.2016 in Kraft getretene E-Health-Gesetz versucht nun, die digitale Vernetzung voranzutreiben. So wurden einerseits telemedizinische Anwendungen, der Medikationsplan und der elektronische Arztbrief erstmals gesetzlich verankert.[44] Andererseits haben die gesetzlichen Krankenversicherungen eine Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) gegründet, die Aufbau und Betrieb der Telematikinfrastruktur übernimmt. Dies hat auch für die Krankenkassen eine besondere Bedeutung. Das E-Health-Gesetz sieht Sanktionen in Form von Mittelkürzungen vor, sofern die Fristen, bis zu denen die Maßnahmen zur flächendeckenden Einführung von ersten Anwendungen der Telematikinfrastruktur abgeschlossen werden müssen, nicht eingehalten werden.

Zudem finden sich in diesem Gesetz die rechtlichen Grundlagen für eine Infrastruktur, die über die elektronische Gesundheitskarte hinaus geht, und für die elektronische Patientenakte, welche einen weiteren Meilenstein in der Entwicklung der Telematikinfrastruktur darstellen soll. In diesem Kontext soll Integrating the Healthcare Enterprise (IHE), eine internationale Initiative von Anwendern und Herstellern mit dem Ziel, die Infrastruktur im Gesundheitswesen zu standardisieren und zu harmonisieren, E-Health auch in Deutschland – ähnlich wie im Nachbarland Österreich – voranbringen.[45] IHE ist bislang im Kontext der digitalen Transformation in Deutschland noch weitgehend unbekannt. Manche Experten sehen darin nur einen zusätzlichen Standard, der nicht benötigt werde. In Österreich jedoch baut das Vernetzungsprojekt „ELGA“ (Elektronische Gesundheits-Akte) auf einer kompletten IHE-konformen Infrastruktur auf. Die IHE geht dabei nach klaren Regeln vor: Sie entwickelt eine Methodik, die für medizinische Prozesse einheitliche Standards mit eindeutigen Gebrauchsanweisungen definiert und vereint Hersteller, Entwickler, Forscher und Nutzer weltweit. Jede Aktivität steht unter

---

[42] vbw, Vorsprung Bayern – Chancen der Digitalisierung für die Gesundheitswirtschaft, S. 7, https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Planung-und-Koordination/2016/Downloads/20160929-VB-Digitalisierung-Gesundheitswirtschaft.pdf (zuletzt abgerufen am 02.08.2017).
[43] Paland/Holland, NZS 2016, 247 f. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[44] Im Einzelnen siehe die Ausführungen unter 3.2.
[45] http://www.optimal-systems.de/2016/06/13/ihe-initiative-oder-standard (zuletzt abgerufen am 02.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

der Prämisse, allen Akteuren zu jeder Zeit und an jedem Ort schnellen Zugriff auf relevante Informationen zu ermöglichen. Sie kann sich daher bei der Gewährleistung einer leistungsfähigen, flächendeckenden, digitalen Infrastruktur als hilfreich erweisen. Darüber hinaus versprechen für die Menge an Daten, die sich im Falle einer ausgebauten Infrastruktur anhäuft, in technischer Hinsicht cloud-basierte Lösungen eine unlimitierte und kosteneffiziente Skalierbarkeit.[46] Sie fördern die Interoperabilität und können einen reibungslosen Datenaustausch ermöglichen.

2.4.2 Informationsaustausch am Beispiel der elektronischen Gesundheitskarte (eGK)

Seit dem 01.01.2015 ist die elektronische Gesundheitskarte deutschlandweit eingeführt. In Zukunft sollen Gesundheitsdaten auf dieser Karte elektronisch zur Verfügung gestellt werden. Ziel ist es, damit die Qualität der medizinischen Versorgung zu verbessern und den Informationsaustausch zwischen Patienten, Ärzten und Krankenkassen zu erleichtern.[47] Sofern der Versicherte dem zustimmt, werden Daten für die Notfallversorgung, der elektronische Arztbrief, Daten zur Prüfung der Arzneimitteltherapiesicherheit (AMTS) sowie das elektronische Rezept auf der eGK digital gespeichert. Die eGK ist – bildlich gesprochen – der Schlüssel für die Telematikinfrastruktur in der Hand des Patienten und Versicherten. Bestandteile der Erprobungsphase der interoperablen eGK sind die Anbindung an das sichere Telekommunikationsnetz der Kassenärztlichen Vereinigungen (KV-SafeNet), die Verknüpfung mit der qualifizierten elektronischen Signatur z.B. zur Erstellung von eRezepten sowie die sichere Kommunikation der Leistungserbringer (KOM-LE). Nur so können medizinische Dokumente rechtssicher unterschrieben und zwischen den Institutionen ausgetauscht werden. Hierfür entwickelt die Industrie einen Konnektor, der durch die gematik auf Basis der Zertifizierung des Bundesamts für Sicherheit in der Informationstechnik zugelassen werden muss. Nach Abschluss dieser Prozesse können Haus- und Fachärzte, Krankenhäuser, Apotheken und auch der Pflege- und Heilsektor angebunden und mithin der Informationsaustausch zwischen allen Beteiligten ermöglicht werden.

Sobald den zugriffsberechtigten Leistungserbringern die technische Infrastruktur flächendeckend zur Verfügung steht, haben die Krankenkassen ihren Versicherten geeignete technische Einrichtungen für einen eigenhändigen Datenzugriff zur Verfügung zu stellen (vgl. § 291a Abs. 5a Satz 5 SGB V). Die gematik arbeitet insoweit bereits an technischen Lösungen wie z.B. in Gestalt einer App, über die in Kombination mit einem geeigneten Lesegerät ein gesicherter Datenzugriff auf einfache Weise erfolgen können soll.[48] Hierüber ist den Patienten ein Lesezugriff auf alle auf der eGK gespeicherten

---

[46] Arvato Bertelsmann, Digitalisierung im deutschen Gesundheitswesen, S. 9.
[47] Elmer, in: Andelfinger/Hänisch, eHealth, 2016, S. 100 ff. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[48] https://www.aerzteblatt.de/nachrichten/74463/Gesundheitskarte-Datenzugriff-der-Patienten-erfordert-komplexe-Loesung (zuletzt abgerufen am 02.08.2017).

Daten sowie ein Schreibzugriff nur für bestimmte Daten, etwa Erklärungen über eine Gewebe- oder Organspende, zu gewähren.

Anfang August 2017 meldeten mehrere Zeitungen, die elektronische Gesundheitskarte „stehe vor dem Aus"; die Bundesregierung wolle das Projekt nach der Bundestagswahl Ende September 2017 für gescheitert erklären[49]. Dem hat das Bundesgesundheitsministerium für Gesundheit mittlerweile.[50] Es bleibt abzuwarten, wie sich die politische Lage gestaltet.

2.4.3 Datenschutz und Datensicherheit

Die Sicherheit und der Schutz der Patientendaten muss im Rahmen der Digitalisierung immer oberste Priorität haben. Bedingt durch die moderne Gesellschaft erheben nicht mehr nur die Institutionen der Leistungserbringer Daten, sondern auch die Patienten selbst. Hauptakteure sind daher indirekt die Patienten und direkt die Ärzte, die Krankenhäuser und auch die Krankenkassen. Die Daten, die im Gesundheitswesen erhoben werden, können in drei Kategorien eingeteilt werden: „New Omics", „Traditional" und „Quantified Self".[51]

„New Omics" beschreiben dabei Daten über das Genom und mikrobiologische sowie metabolische Eigenschaften, die als Profile mit automatisierten Methoden erhoben werden.

„Traditional" nennt man die Verarbeitung von diagnostischen und therapeutischen Daten durch Krankenhäuser, Ärzte und Krankenkassen.

„Quantified Self" bezeichnet die Erhebung von gesundheitsbezogenen Daten durch den Patienten selbst, vorzugsweise durch die Nutzung des zweiten Gesundheitsmarktes. Gerade die aufgrund der zuletzt angesprochenen Kategorie insgesamt stetig zunehmende Masse an Daten erfordert die rechtliche wie technische Gewährleistung von Datenschutz und Datensicherheit in besonders hohem Maße. Damit einher geht die Verpflichtung aller Akteure zu einem sensiblen Umgang mit den beschriebenen Datenmassen.[52]

---

[49] Vgl. http://www.focus.de/gesundheit/news/elektronische-gesundheitskarte-massive-zweifel-an-zukunft-der-karte_id_7440534.html, zuletzt abgerufen am 10.8.2017.
[50] https://www.welt.de/regionales/bayern/article167457982/Elektronische-Gesundheitskarte-nicht-vor-dem-Aus.html, zuletzt abgerufen am 10.8.2017.
[51] Timm, MedR 2016, 681, 688.
[52] Zu den Einzelheiten siehe unter 3.1.2 sowie 4.

3 Fragmente eines E-Health-Rechts

Der vorhandene Rechtsrahmen

Für das Verständnis der ausgewählten Problemfelder Vernetzung, Datenschutz und Big Data[53] muss zunächst der vorhandene Rechtsrahmen für den Bereich digitalisiertes Gesundheitswesen erläutert werden. Hierbei sollen neben der vorhandenen – fragmentarischen – Regulierung durch das E-Health-Gesetz auch noch bestehende Desiderate aufgezeigt werden, ebenso wie übergeordnete Handlungsmaximen.

3.1 Is‘ was, doc? Heterogenität der rechtlichen Anknüpfung

E-Health gewinnt immer mehr an Bedeutung. Der geschätzte Umsatz in diesem Bereich beträgt im Jahr 2017 knapp 400 Millionen Euro.[54] Dennoch mangelt es an einer einheitlichen rechtlichen Regulierung. Auch das „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen“ (E-Health-Gesetz) vom 21.12.2015[55], welches am 01.01.2016 in Kraft trat, kann und soll auch nicht die gesamte Digitalisierung im Gesundheitswesen regulieren. In Anbetracht der Vielzahl der Lebensbereiche, die durch das zunehmend digitalisierte Gesundheitswesen berührt wird, lassen sich spezialgesetzliche Regelungen nicht vermeiden. Eine exakte Prüfung, welches Gesetz anzuwenden ist, wird auch in Zukunft notwendig sein. Von entscheidender Bedeutung sind dabei zunächst der konkrete Einzelfall sowie der jeweils handelnde Teilnehmer aus dem Gesundheitswesen.

3.1.1 Die Beteiligten im Gesundheitswesen

Die komplexen rechtlichen Strukturen im Gesundheitswesen ergeben sich nicht zuletzt aus dem Umstand, dass hier verschiedene Akteure in unterschiedlichsten Rechtsbeziehungen zueinander stehen. Zunächst ist – neben den politischen Akteuren auf Bundes-, Landes- und Kommunalebene – zwischen den Leistungsberechtigten, den Leistungserbringern und den Leistungsträgern zu unterscheiden.

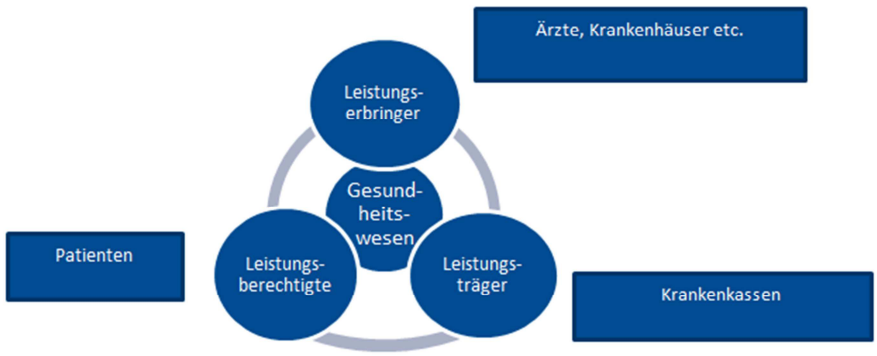
[53] Siehe hierzu unter 4.
[54] https://de.statista.com/outlook/312/137/ehealth/deutschland#market-revenue (zuletzt abgerufen am 02.08.2017).
[55] BGBl. I, S. 2408.

Zu den Leistungsträgern zählen die gesetzlichen und privaten Krankenkassen. Die Leistungsansprüche des Versicherten, d.h. des Leistungsberechtigten, gegenüber den gesetzlichen Krankenkassen sind allen voran im SGB V sowie in den Rechtsverordnungen und Satzungen der Krankenkasse festgelegt. Im Bereich der privaten Krankenversicherungen finden sich – neben den allgemeinen Bestimmungen des BGB – die maßgeblichen Vorschriften im zweiten Teil des Versicherungsvertragsgesetzes (VVG).

Zu den Aufgaben der medizinischen Leistungserbringer zählen diejenigen, die die Krankenkassen nicht selbst leisten können.[56] Zu der Gruppe der Leistungserbringer zählen unter anderem Ärzte, Krankenhäuser, Psychotherapeuten, Physiotherapeuten, Pflegedienste, Apotheken, Heilpraktiker sowie sonstige Leistungserbringer. Das Recht der Leistungserbringer wird ebenfalls maßgeblich durch das SGB V bestimmt, weitere speziell zu beachtende Bestimmungen finden sich in den jeweiligen Landeskrankenhausgesetzen sowie den Berufsordnungen der Ärztekammern.

Zu beachten ist weiterhin, dass bis auf wenige Ausnahmen, wie z.B. der vor- und nachstationären Behandlung im Krankenhaus (§ 115a SGB V), strikt zwischen stationärer und ambulanter Versorgung getrennt wird.[57]

Abbildung 3
Beteiligte im Gesundheitswesen



[56] Becker/Kingreen, SGB V, 5. Aufl. 2017, § 69 Rn. 25 f.
[57] Kleinke, in: Saalfrank, Medizin- und Gesundheitsrecht, 6. EL 2016, § 3 Rn. 45.

3.1.2 Maßgebliche verfassungsrechtliche Wertungen

Bei der Frage der rechtlichen Anknüpfungspunkte ist zunächst auf verfassungsrechtliche Wertungen einzugehen. Von Bedeutung ist in diesem Kontext insbesondere das Spannungsverhältnis zwischen der Forschungsfreiheit aller Beteiligten aus Art. 5 Abs. 3 GG, der Berufsfreiheit der Leistungserbringer und Leistungsträger aus Art. 12 Abs. 1 GG und dem Recht auf informationelle Selbstbestimmung des Patienten aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.[58] Schutz erfährt der Patient mit Blick auf seine personenbezogenen Daten durch das Recht auf informationelle Selbstbestimmung. Auf einfachgesetzlicher Ebene konkretisieren dieses die Datenschutzgesetze[59] sowie etwa auch die Vorschrift des § 203 StGB mit Blick auf die ärztliche Schweigepflicht. Das Recht auf informationelle Selbstbestimmung umfasst weiterhin auch das sogenannte „Recht auf Nichtwissen“,[60] welches gerade durch den Bereich der prädiktiven genetischen Diagnostik gefährdet wird.[61] Dabei ist allerdings zu beachten, dass die informationelle Selbstbestimmung kein uneingeschränktes Recht ist, sondern mit legitimen Interessen und damit insbesondere mit den anfangs genannten Grundrechten der Leistungserbringer und -träger in Ausgleich zu bringen ist. Dazu können allen voran die unter 3.4 genannten datenschutzrechtlichen Grundsätze herangezogen werden.[62] Die Wahrung des informationellen Selbstbestimmungsrechtes obliegt nicht nur dem Staat, auch private Stellen sind gegenüber dem Bürger durch die sogenannte mittelbare Drittwirkung der Grundrechte verpflichtet.[63] So ergibt sich beispielsweise aus dem informationellen Selbstbestimmungsrecht im Zusammenwirken mit der ärztlichen Schweigepflicht aus § 203 StGB, dass der Arzt Patientendaten nicht unbefugt an Dritte weiterleiten darf.[64]

Mit seinem Urteil vom 27.08.2008 hat das Bundesverfassungsgericht überdies auf den Fortschritt im Technologiebereich reagiert und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anerkannt (sogenanntes IT-Grundrecht).[65] Dieses leitet sich ebenfalls aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ab. Von seinem Schutzbereich sind insbesondere Systeme erfasst, die für sich oder aufgrund technischer Vernetzung personenbezogene Daten eines Einzelnen enthalten können und bei denen ein Zugriff auf das jeweilige System einen Einblick in die Lebensgestaltung des Nutzers ermöglicht oder die Erstellung eines Persönlichkeitsbildes erlaubt.[66] Das Grundrecht soll die Vertraulichkeit der durch ein System er-

---

[58] Hoeren, Big Data und Recht, 2014, S. 132; Ludwig, in: Neuroth/Strathmann/Oßwald/Scheffel/Klump, Langzeitarchivierung von Forschungsdaten, 2012, Kap. 12, S. 247.
[59] Siehe hierzu näher unter 3.1.2.
[60] Di Fabio, in: Maunz-Dürig, GG, 72. EL 2014, Art. 2 Rn. 192.
[61] Damm, MedR 2011, 7, 8.
[62] Dorschel, Praxishandbuch Big Data, 2015, S. 168.
[63] Weichert, in: Langkafel, Big Data in Medizin und Gesundheitswirtschaft, 2014, S. 164.
[64] König/Junge, GuP 2015, 132, 135.
[65] BVerfG, Urt. v. 27.02.2008 - 1 BvR370/07, 1 BvR 595/07 (Online-Durchsuchung).
[66] Böckenförde, JZ 2008, 925.

zeugten, verarbeiteten und gespeicherten Daten schützen sowie einen heimlichen Zugriff wie z.B. durch eine Online-Durchsuchung unterbinden.[67]

Nicht außer Acht zu lassen ist im Rahmen der verfassungsrechtlichen Wertungen ferner der Gesichtspunkt, dass neue Technologien im E-Health-Bereich und die damit verbundenen Datenverarbeitungen auch dazu geeignet sein können, zu einer besseren gesundheitlichen Versorgung der Bevölkerung beizutragen. Insoweit trifft den Staat durch das in Art. 2 Abs. 2 Satz 1 GG verankerte Grundrecht auf Leben und körperliche Unversehrtheit zwar nicht die Pflicht, ein allgemeines staatliches System der Gesundheitsvorsorge vorzuhalten, jedoch bedarf es einer Infrastruktur gesundheitlicher Mindestversorgung.[68] Aus diesem Grundrecht und aus dem Sozialstaatsprinzip (Art. 20 Abs. 1, 28 Abs. 2 Satz 1 GG) ergibt sich zudem die staatliche Pflicht, jedermann ohne Rücksicht auf Alter und Einkommen Zugang zu notwendiger medizinischer Versorgung zu gewähren.[69] Hierzu können die genannten Technologien einen positiven Beitrag leisten.

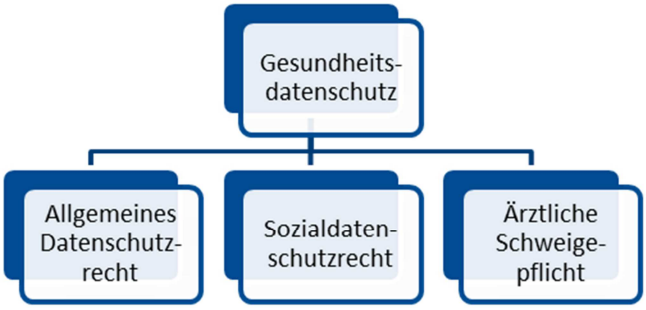
3.1.3 Datenschutzrechtliche Bestimmungen

Im Bereich der E-Health-Anwendungen soll – ausgehend von den dargestellten verfassungsrechtlichen Wertungen – stets der Datenschutz im Mittelpunkt stehen.[70] Neben den neuen Vorgaben des E-Health-Gesetzes, z.B. im Bereich der elektronischen Gesundheitskarte (§ 291a SGB V), sind weitere umfangreiche datenschutzrechtliche Bestimmungen zu beachten. Diese finden sich in einer Vielzahl von Gesetzen, welche abhängig vom jeweiligen Akteur einschlägig sein können. Zur Klärung der jeweils einschlägigen Norm bietet sich zunächst eine Aufteilung in das allgemeine Datenschutzrecht, das besondere (Sozial-)Datenschutzrecht und die Regelungen zur ärztlichen Schweigepflicht an:[71]

Abbildung 4
Normative Verankerung des Gesundheitsdatenschutzes

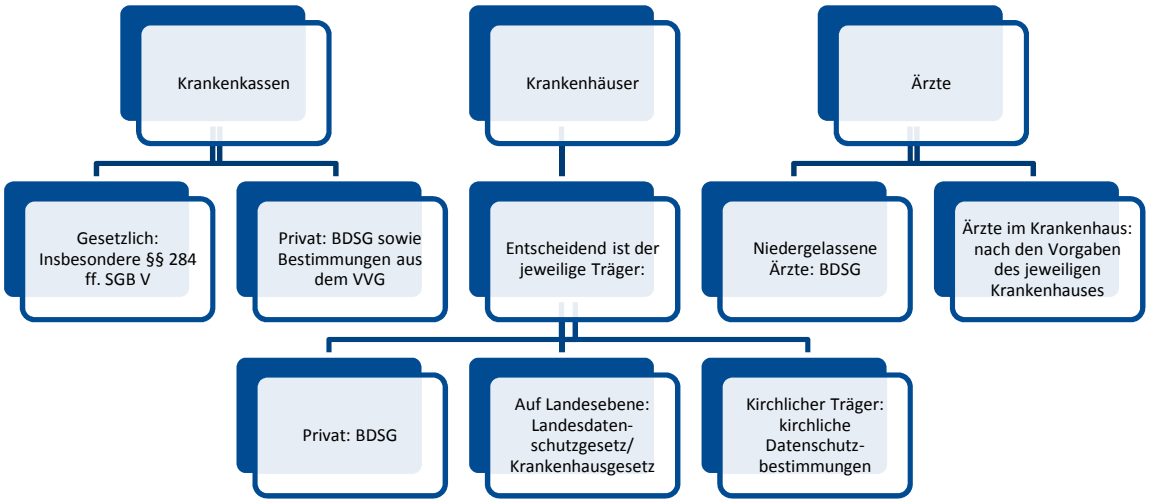
---

[67] Schmidt, in: Erfurter Kommentar zum Arbeitsrecht, 17. Aufl. 2017, GG, Art. 2 Rn. 43.
[68] Di Fabio, in: Maunz/Dürig, GG, 79. EL 2016, Art. 2 Abs. 2 Satz 1 Rn. 46 m.w.N.
[69] Steiner, in: Spickhoff, Medizinrecht, 2. Aufl. 2014, Art. 20 GG Rn. 5.
[70] So Bundesgesundheitsminister Herman Gröhe, abrufbar unter: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-gesetz/e-health.html (zuletzt abgerufen am 02.08.2017).
[71] Buchner, MedR 2016, 660, 661.



Welche Säule im konkreten Fall einschlägig ist, richtet sich danach, wer die Daten verwendet. Beispielsweise sind im Bereich der gesetzlichen Krankenkassen die Vorgaben des SGB V gemäß den §§ 284 ff. SGB V einschlägig, während der Datenschutz in den Krankenhäusern oftmals durch die jeweiligen landesrechtlichen Krankenhausgesetze bestimmt wird. Für den Bereich der Ärzte kommt in der Regel das Bundesdatenschutzgesetz (BDSG) zur Anwendung.

Abbildung 5
Rechtsquellen des Datenschutzrechts im E-Health-Sektor



Von besonderer Bedeutung wird in Zukunft die Datenschutz-Grundverordnung sein, die ab dem 25.05.2018 gilt. Mit der Datenschutz-Grundverordnung werden im medizinischen Bereich die Vorgaben der Datenschutz-Richtlinie[72] im Wesentlichen fortgeführt und ergänzt.[73]

Die Datenschutz-Grundverordnung definiert Gesundheitsdaten in Art. 4 Nr. 15. Demnach sind Gesundheitsdaten *„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen."* Die Verarbeitung dieser Daten ist nach den Vorgaben der Datenschutz-Grundverordnung grundsätzlich verboten (Art. 9 Abs. 1 Datenschutz-Grundverordnung). Sie ist nur dann erlaubt, wenn entweder die betroffene Person ausdrücklich eingewilligt hat oder ein gesetzlicher Erlaubnistatbestand vorliegt (Art. 9 Abs. 2 Datenschutz-Grundverordnung). Erwägungsgrund 52 der Datenschutz-Grundverordnung führt diesbezüglich aus, dass die Verarbeitung von Gesundheitsdaten insbesondere dann zulässig sein soll, wenn sie für die Gewährleistung der öffentlichen Gesundheit und der Verwaltung der Gesundheitsversorgung notwendig ist.

3.1.4 Weitere bundesrechtliche Vorgaben zur Digitalisierung im Gesundheitswesen

Bei der rechtskonformen Umsetzung und Durchführung von E-Health-Anwendungen sind zudem oftmals weitere spezielle („bereichsspezifische") Vorgaben zu beachten. Abhängig vom jeweiligen Akteur können Regelungen aus den unterschiedlichsten Bereichen für die Digitalisierung im Gesundheitswesen von Bedeutung sein. Allerdings sind auch allgemeine Gesetze wie das BGB oder das StGB von Relevanz. Bereichsspezifische Normen, die bei der Digitalisierung im Gesundheitswesen zu beachten sind, sind z.B. das Gendiagnostikgesetz (GenDG), das Heilmittelwerbegesetz (HWG), das Infektionsschutzgesetz (IfSG), das Medizinproduktegesetz (MPG), die Röntgenverordnung (RöV) oder die Strahlenschutzverordnung (StrlSchV). Daneben spielen auch kostenrechtliche Regelungen wie z.B. die Gebührenordnung für Ärzte (GOÄ) eine Rolle.

Beispiel: Vorgaben der Röntgenverordnung zur Teleradiologie

Die Teleradiologie kommt vor allem dann zum Einsatz, wenn eine radiologische Befundung notwendig ist, aber aus zeitlichen, personellen oder technischen Gründen am

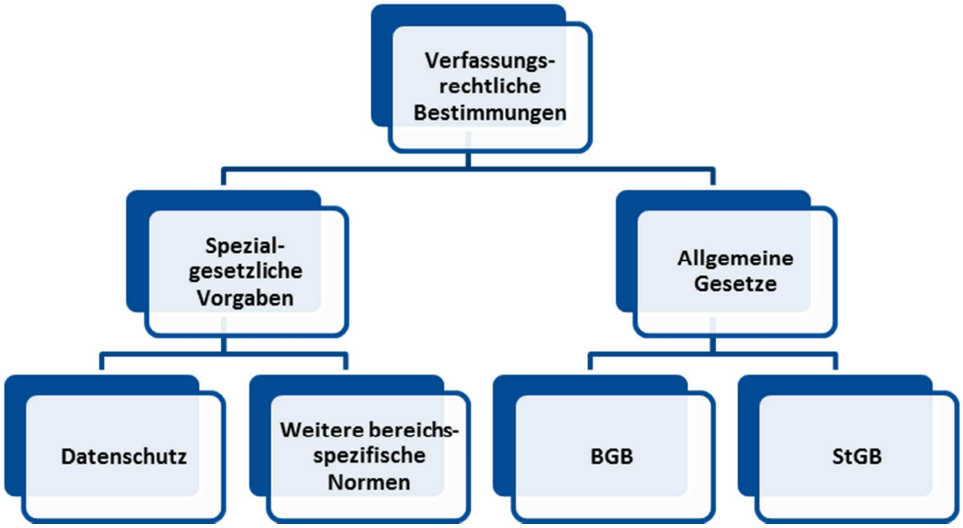
---

[72] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281, S. 31-50.
[73] Spindler, MedR 2016, 691, 694.

Behandlungsort eigentlich nicht durchgeführt werden kann. Von besonderer Bedeutung ist dabei der Fall, dass die Untersuchung (in einem Krankenhaus) außerhalb der Dienstzeiten des Radiologen erfolgen muss. In dieser Konstellation werden die zunächst durch das Krankenhaus erstellten Bilder an einen weiteren (externen) Radiologen übermittelt.[74] Die Teleradiologie kann in solchen Fällen gem. § 3 Abs. 4 RöV zulässig sein, um zeitliche Verzögerungen bei der Untersuchung sowie Transportrisiken zu vermeiden.[75]

Die Rechtsquellen der Digitalisierung im Gesundheitswesen lassen sich zusammenfassend wie folgt veranschaulichen:

Abbildung 6
Rechtsquellen der Digitalisierung im Gesundheitswesen



3.2 Was gilt? Regulierungen durch das E-Health-Gesetz

3.2.1 Allgemeines zum E-Health-Gesetz

Das am 01.01.2016 in Kraft getretene „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen“ (E-Health-Gesetz) hat zum Ziel, den Informati-

---

[74] Cramer/Dahm/Henkel, MedR 2015, 392, 394.
[75] BR-Drs. 230/02, S. 75.

onszugriff sowie die Kommunikation zwischen den Leistungserbringern zu erleichtern und dadurch eine Qualitätssteigerung im Bereich der medizinischen Versorgung zu erzielen.[76] Die Vorschriften des E-Health-Gesetzes stellen sozusagen einen Fahrplan dar, mittels dessen die Digitalisierung im Gesundheitswesen Schritt für Schritt vorangetrieben werden soll.[77] Mit dem Gesetz wurden überwiegend die Vorschriften des SGB V abgeändert.

Die Vernetzung erfolgt auf drei verschiedenen Stufen.[78] Jede dieser Stufen stellt die Wirtschaft vor neue Herausforderungen. Die erste Stufe sieht vor, die auf bestehender Technik basierenden Anwendungen zu fördern. Hierzu zählen insbesondere der Medikationsplan, der elektronische Arztbrief und telemedizinische Anwendungen (wie etwa die Online-Sprechstunde). Die neuen SGB-Vorschriften zum Medikationsplan sowie zum E-Arztbrief sehen zudem bereits vor, diese Anwendungen zu einem späteren Zeitpunkt in die Telematikinfrastruktur zu integrieren. Auf der zweiten Stufe etabliert das E-Health-Gesetz konkrete Schutzmechanismen, um den Ausbau der Telematikinfrastruktur zu sichern. Im Rahmen der dritten Stufe soll die Telematikinfrastruktur zur zentralen Infrastruktur im digitalen Gesundheitswesen ausgebaut werden.[79] Einen wichtigen Baustein bildet insoweit die elektronische Patientenakte. Für Aufbau und Betrieb dieser Telematikinfrastruktur ist die Anfang 2005 von den Spitzenverbänden des deutschen Gesundheitswesens gegründete Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zuständig. Gesellschafter der gematik sind mit 50 Prozent der Anteile unter anderem die Bundesärztekammer sowie die Deutsche Krankenhausgesellschaft, die anderen 50 Prozent entfallen auf den Bund der Krankenkassen (§ 291b Abs. 2 Nr. 1 SGB V).

Die vorrangigen Ziele des E-Health-Gesetzes:[80]

- *Der Anwendungsbereich der elektronischen Gesundheitskarte soll zügig mit weiterführenden Anwendungen erweitert werden.*

- *Um eine sichere Kommunikation im Gesundheitswesen gewährleisten zu können, soll eine zentrale Telematikinfrastruktur eingerichtet und diese für weitere Leistungserbringer geöffnet werden.*

---

[76] Bergmann, MedR 2016, 497.
[77] Bundesministerium für Gesundheit, Das E-Health-Gesetz, 28.12.2015, https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-gesetz/e-health.html (zuletzt abgerufen am 02.08.2017).
[78] Paland/Holland, NZS 2016, 247, 248.
[79] BT-Drs. 18/5293, S. 2.
[80] Vgl. den Referentenentwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen v. 13.01.2015, S. 1, https://extdsb.files.wordpress.com/2015/01/re_e-health-gesetz1.pdf (zuletzt abgerufen am 02.08.2017).

- *Die Gesellschaft für Telematik soll mit weitergehenden Kompetenzen ausgestattet und strukturell verbessert werden.*

- *Die informationstechnischen Systeme im Gesundheitswesen sollen interoperabel gestaltet werden.*

- *Telemedizinische Leistungen sollen ausgebaut und gefördert werden.*

3.2.2 Die wichtigsten Regelungen des E-Health-Gesetzes im Überblick

Kapitelübersicht

3.2.2.1 Der Medikationsplan, § 31a SGB V

Gem. § 31a Abs. 1 Satz 1 SGB V haben Versicherte, die gleichzeitig mindestens drei verordnete Arzneimittel anwenden, seit dem 01.10.2016 einen Anspruch auf Erstellung und Aushändigung eines Medikationsplans in Papierform. Mit dieser Regelung möchte der Gesetzgeber den Gefahren, die durch Wechselwirkungen bei der Einnahme mehrerer Medikamente entstehen können, entgegenwirken.[81] Es ist vorgesehen, dass der Medikationsplan ab 2018 in digitaler Form auf der elektronischen Gesundheitskarte gespeichert wird und von dieser abgerufen werden kann.[82]

---

[81] Starnecker/Kuhls, jurisPR-ITR 10/2015, Anm. 2.
[82] Bundesministerium für Gesundheit, Das E-Health-Gesetz, 28.12.2015, http://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-gesetz/e-health.html (zuletzt abgerufen am 02.08.2017).

Der Medikationsplan nach den Vorgaben des § 31a SGB V:[83]

Freiwilliger Anspruch auf Erstellung und Aushändigung ab der gleichzeitigen Einnahme/Anwendung von mindestens drei verordneten Medikamenten.

Inhalt des Medikationsplans:

- *Verschreibungspflichtige Arzneimittel*
- *Gegebenenfalls auch die Einnahme von nicht verschreibungspflichtigen Medikamenten*
- *Anwendungshinweise*
- *Gegebenenfalls weitere relevante Medizinprodukte*

Praxistipp: Chancen für die Wirtschaft

Der Medikationsplan kann nicht nur gefährliche Wechselwirkungen vermeiden, er kann ebenfalls dazu beitragen, dass Medikamente wie verordnet eingenommen werden. Non-Compliance, also die nicht verordnungsgemäße Einnahme der verschriebenen Medikamente kann zu enormen gesundheitlichen wie wirtschaftlichen Schäden führen.[84] Experten gehen sogar davon aus, dass dies eines der größten Probleme im Gesundheitssektor darstellt.[85] Entwicklungen aus der Wirtschaft könnten dazu beitragen, den Medikationsplan, z.B. mit einer Erinnerungsfunktion, auf dem Smartphone des Anwenders abrufbar zu machen. Auch in der freiwilligen Verknüpfung mit weiteren Informationen über den Nutzer, z.B. betreffend seine Ernährung, können weitere Potenziale liegen.

3.2.2.2 Der elektronische Arztbrief, § 291f SGB V

Um die elektronische Kommunikation zwischen den beteiligten Vertragsärzten und Einrichtungen zu fördern, erhalten diese unter der Voraussetzung, dass sie einen elektronischen Heilberufsausweis erworben haben, ab 2017 pro übermittelten elektronischen Brief einen Pauschalbetrag in Höhe von 55 Cent.[86] Der finanzielle Anreiz bei der Verwendung des elektronischen Arztbriefes soll dazu beitragen, die Telematikinfrastruktur auszubauen. Die Regelung des § 291f SGB V stellt daher nur eine Übergangs-

---

[83] Checkbox nach: Kassenärztliche Bundesvereinigung, Informationen für die Praxis – Arzneimitteltherapie, S. 5, http://www.kbv.de/media/sp/2016_09_29_Praxisinformation_Medikationsplan.pdf (zuletzt abgerufen am 02.08.2017).
[84] Rieß, NZS 2014, 12.
[85] Metzger, Adherence – Dreimal täglich! Ist das denn so schwer? PZ online, Ausgabe 42/2013.
[86] Scholz, in: BeckOK SozR, SGB V, 45. Edition, Stand 01.06.2017, § 291f Rn. 1.

lösung dar und gilt folglich nur im Jahr 2017.[87] Als problematisch erwies sich Anfang 2017 der Umstand, dass von den 172 für den vertragsärztlichen Gebrauch zugelassenen Praxis-EDV-Systemen nur neun Systeme die erforderliche Zertifizierung für den E-Arztbrief aufwiesen.[88] Inzwischen hat sich diese Zahl jedoch deutlich erhöht.[89] Ein erster Praxistest der KV Telematik GmbH, einer Tochtergesellschaft der Kassenärztlichen Bundesvereinigung, hat eine hohe Zufriedenheit mit dem elektronischen Arztbrief unter den beteiligten Ärzten ergeben.[90]

Weiterhin soll die Bestimmung die Verbreitung des elektronischen Heilberufsausweises fördern, da dieser ab dem 01.01.2018 für weitere Anwendungen, wie z.B. den elektronischen Medikationsplan, vorgesehen ist.[91]

3.2.2.3 Online-Videosprechstunden und die konsiliarische Befundbeurteilung, § 87 Abs. 2a in Verbindung mit § 291g SGB V

Auf Grundlage des E-Health-Gesetzes soll im Jahr 2017 der *Einheitliche Bewertungsmaßstab* zur Vergütung ärztlicher Leistungen um den Bereich der Online-Sprechstunden als auch der konsiliarischen Röntgenbefundbeurteilung ergänzt werden. Damit soll eine erste Grundlage für eine flächendeckende Telemedizin-Versorgung im diagnostischen Bereich geschaffen werden. Pilotprojekte wie „patentius“[92] zeigen das enorme wirtschaftliche Potential in diesem Bereich.

Hinweis

Im Bereich der Telemedizin ist § 7 Abs. 4 der Musterberufsordnung für die in Deutschland tätigen Ärzte zu beachten. Demnach ist bei telemedizinischen Verfahren zu gewährleisten, dass der Arzt den Patienten unmittelbar behandelt. Jedenfalls die reine Online-Behandlung ist daher nach aktueller Rechtslage ausgeschlossen.

---

[87] Paland/Holland, NZS 2016, 247, 249.
[88] Höhl, ÄrzteZeitung, E-Arztbrief: Förderung mit Hindernissen, 20.01.2017, https://www.aerztezeitung.de/praxis_wirtschaft/e-health/gesundheitskarte/article/927790/e-arztbrief-foerderung-hindernissen.html (zuletzt abgerufen am 03.08.2017).
[89] https://www.kv-telematik.de/index.php?id=222 (zuletzt abgerufen am 03.08.2017).
[90] Höhl. ÄrzteZeitung, E-Arztbrief besteht den Praxistest, 27.04.2017, https://www.aerztezeitung.de/praxis_wirtschaft/e-health/article/934433/e-health-e-arztbrief-besteht-praxistest.html?sh=9&h=394363253 (zuletzt abgerufen am 03.08.2017).
[91] Scholz, in: BeckOK SozR, SGB V, 45. Edition, Stand 01.06.2017, § 291f Rn. 1.
[92] Über „patentius“ können bereits Online-Sprechstunden durchgeführt werden. Für Patienten ist die Benutzung des Services kostenlos, Ärzte hingegen müssen einen kostenpflichtigen Account anlegen. Die Gebühren für die jeweilige Online-Sitzung können die Ärzte sodann individuell festlegen, vgl. https://www.patientus.de/de/ (zuletzt abgerufen am 02.08.2017).

Praxistipp: Chancen für die Wirtschaft

Annähernd 45 Prozent der deutschen Patienten stehen der digitalen Sprechstunde offen gegenüber.[93] Für Ärzte, die einen solchen Service anbieten, ergeben sich daher Wettbewerbsvorteile. In diesem Bereich werden sich bei Aufbau und Unterhalt der entsprechenden telemedizinischen Infrastruktur zukünftig weitreichende Kooperationsmöglichkeiten zwischen dem Gesundheitswesen und der Wirtschaft eröffnen.

3.2.2.4 Funktionserweiterungen der elektronischen Gesundheitskarte

Das E-Health-Gesetz hat das Ziel, möglichst schnell förderliche Anwendungen für die elektronische Gesundheitskarte zu etablieren. Um dies zu erreichen, wurden die Vorschriften des SGB V, die sich mit der elektronischen Gesundheitskarte befassen (§§ 291 ff. SGB V), angepasst, erweitert und mit Fristen versehen, innerhalb derer bestimmte Anwendungen implementiert werden müssen.

In diesem Zusammenhang dürften für die Wirtschaft vor allem die freiwilligen Anwendungen auf der Gesundheitskarte interessant sein. Zu diesen freiwilligen Anwendungen zählen:

- Notfalldaten (notfallrelevante Daten etwa über Arzneimittelunverträglichkeiten)
- der elektronische Arztbrief (Befunde, Diagnosen, Therapieempfehlungen etc.)
- Daten zur Prüfung der Arzneimitteltherapiesicherheit und der E-Medikationsplan
- die elektronische Patientenakte (Arztbriefe und Impfungen)
- das elektronische Patientenfach

Die Daten für die Notfallversorgung sollen ab 2018 – wie bereits erwähnt – freiwillig auf der elektronischen Gesundheitskarte gespeichert werden. Freiwilligkeit bedeutet, dass das Erheben, Verarbeiten oder Nutzen dieser Daten nur mit Einverständnis des Versicherten zulässig ist (§ 291a Abs. 5 SGB V). Im Notfall kann auf diese Daten ohne nochmalige Autorisierung des Versicherten zugegriffen werden, für andere Fälle darf auf diese Daten nur zurückgegriffen werden, wenn sie zur Versorgung des Versicherten erforderlich sind und die Nutzung dieser Daten mit dem protokollierten Einverständnis des Nutzers erfolgt (§ 291 Abs. 5 Satz 3 SGB V). Sinn und Zweck der Regelung ist es, im Ernstfall sämtliche notfallrelevanten Informationen etwa über Allergien, Arzneimittelunverträglichkeiten und Vorerkrankungen schnell zur Verfügung zu haben. Damit die Daten auch tatsächlich im Notfall zur Verfügung stehen, müssen sie daher so auf der Gesundheitskarte hinterlegt werden, dass sie auch ohne Zutun des Patienten abrufbar sind. Hier besteht natürlich ein Missbrauchsrisiko (Stichwort: Datensicher-

[93] Bertelsmann Stiftung, Spotlight Gesundheit 11/2015 – Video-Sprechstunden, S. 2.

heit). Die Frage der zivilrechtlichen Verantwortlichkeit im Rahmen des Einsatzes der elektronischen Gesundheitskarte ist noch nicht abschließend durch die Rechtsprechung geklärt. Bis die Gerichte insoweit mehr Rechtssicherheit geschaffen haben, sollten die bestehenden richterrechtlichen Haftungsgrundsätze für die Entscheidung möglicher Haftungsfälle im Zusammenhang mit dem Einsatz von Informations- und Kommunikationstechnik herangezogen werden.[94] Herausforderung und Chance zugleich für die Wirtschaft besteht nunmehr darin, sich gegen mögliche (neue) Haftungsrisiken im Umgang mit der elektronischen Gesundheitskarte entsprechend abzusichern. Diese Aspekte bereits im Rahmen der Softwareentwicklung (Stichwort: Security by design[95]) zu berücksichtigen, erscheint hierbei besonders zielführend.

Das E-Health-Gesetz fördert ebenfalls die Einführung der elektronischen Patientenakte.[96] § 291a Abs. 5c SGB V verpflichtet die gematik, bis zum 31.12.2018 „*die erforderlichen Voraussetzungen dafür zu schaffen, dass Daten über Patienten in einer elektronischen Patientenakte […] bereitgestellt werden können.“* Auf dieser Grundlage soll die elektronische Patientenakte, die von einer Mehrheit der Patienten gewünscht wird,[97] zeitnah umgesetzt werden. Die gematik muss dafür sorgen, dass die Patientendaten (Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen) in der elektronischen Patientenakte für die Patienten bereitgestellt werden können. Mit Hilfe ihrer elektronischen Patientenakte können die Patienten dann die behandelnden Personen über ihre wichtigsten Gesundheitsdaten informieren.

---

[94] Bales/von Schwanenflügel, NJW 2012, 2475, 2476.
[95] Vgl. hierzu Schild, heise Developer, Sichere Softwareentwicklung nach dem „Security by Design“-Prinzip, 19.08.2009, https://www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html (zuletzt abgerufen am 03.08.2017).
[96] BT-Drs. 18/6905, S. 60.
[97] Repräsentative TNS Emnid Umfrage vom September 2016, durchgeführt im Auftrag der Verbraucherzentrale Bundesverband, http://www.vzbv.de/infografik/infografik-die-digitalisierung-der-gesundheitsversorgung-aus-patientensicht (zuletzt abgerufen am 02.08.2017).

Ergänzend zur elektronischen Gesundheitskarte soll ein elektronisches Patientenfach geschaffen werden, um die Versicherten stärker an der Digitalisierung im Gesundheitswesen teilhaben zulassen.[98] Dem Bundesverband Bitkom zufolge wünschen 87 Prozent der Bundesbürger unmittelbaren Zugriff auf die sie betreffenden Gesundheitsdaten.[99] Das Patientenfach soll dem Patienten die Möglichkeit einräumen, den Überblick über seine Gesundheitsdaten zu behalten und diese zugleich mit eigens generierten Daten, z.B. über eine entsprechende App, zu ergänzen. Auch hinsichtlich dieses Faches ist die gematik verpflichtet, die erforderlichen Voraussetzungen bis Ende 2018 zu schaffen, sodass der Patient die Daten jederzeit einsehen kann, § 291b Abs. 1 Satz 12 SGB V.

Praxistipp: Chancen für die Wirtschaft

Die Einführung der elektronischen Patientenakte und des elektronischen Patientenfachs eröffnet zahlreiche Kooperationsmöglichkeiten zwischen den Akteuren im Gesundheitswesen und den Unternehmen. Unter Beachtung der Vorgaben des Datenschutzes könnte durch die elektronische Patientenakte in Kombination mit dem Patientenfach grundsätzlich ein Gesundheitsdaten-Pool entwickelt werden, der für alle Beteiligten nutzbringend verwendet werden könnte. In jedem Fall empfiehlt sich insoweit jedoch die Einholung qualifizierten Rechtsrates, um juristische Nachteile zu vermeiden und bereits bei der technischen Umsetzung auf Datenschutzkonformität zu achten (Stichwort: Privacy by design).

Als Beispiel für eine verpflichtende Anwendung kann das Versichertenstammdaten-Management dienen. Mit der Einführung des § 291 Abs. 2b SGB V werden die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Einrichtungen und Zahnärzte verpflichtet, die auf der elektronischen Gesundheitskarte gespeicherten Versichertenstammdaten online mit denen der Versicherung abzugleichen und gegebenenfalls zu aktualisieren. Die Verpflichtung besteht, sobald die Gesellschaft für Telematik (gematik) die notwendige Infrastruktur dafür bereithält und soll letztlich die Vernetzung der Beteiligten durch die Telematikinfrastruktur vorantreiben.[100] Die dazu erforderlichen Maßnahmen hatte die gematik ursprünglich bis zum 30.06.2016 durchzuführen. Diese Frist wurde daraufhin mittels Rechtsverordnung des Bundesministeriums für Gesundheit bis zum 30.06.2017 verlängert (vgl. § 291 Abs. 2b Satz 9 SGB V). Am 01.06.2017

---

[98] BT-Drs. 18/6905, S. 60.
[99] Bitkom, Patienten wollen Zugang zu ihren Gesundheitsdaten, https://www.bitkom.org/Presse/Presseinformation/Patienten-wollen-Zugang-zu-ihren-Gesundheitsdaten.html (zuletzt abgerufen am 02.08.2017).
[100] Paland/Holland, NZS 2016, 247, 250.

wurde seitens der gematik nach Festlegung der Architektur der Telematikinfrastruktur sowie der Sicherheits- und Betriebskonzepte die Freigabe für den Online-Produktivbetrieb erteilt, womit die Industrie zur Einreichung ihrer Produkte zur Zulassung aufgefordert wurde.[101]

Vom Ausbau der Telematikinfrastruktur sollen in Zukunft auch Anwendungen erfasst werden, die keinen Bezug zur elektronischen Gesundheitskarte haben. Zudem sollen auch weitere, bisher nicht erfasste Leistungserbringer auf diese zugreifen können.[102]

Praxistipp: Chancen für die Wirtschaft

Sowohl beim Ausbau als auch bei der Nutzung der Telematikinfrastruktur können Unternehmen partizipieren und davon profitieren. Bei der Entwicklung und dem Ausbau der Infrastruktur setzt die gematik auf einen engen Austausch mit der Industrie.[103] Letztlich wird eine gut ausgebaute digitale Infrastruktur aber auch zum Standortfaktor für die Unternehmen in ihrer Funktion als Arbeitgeber.[104]

3.2.2.5 Die Telematikinfrastruktur als zentrale Infrastruktur im Gesundheitswesen

Grundlage für die Einführung digitaler Systeme wie die elektronische Patientenakte ist eine umfassende digitale Infrastruktur im Gesundheitswesen. Zur Förderung der Interoperabilität zwischen informationstechnischen Systemen war die gematik bis zum 30.06.2017 verpflichtet, ein elektronisches Interoperabilitätsverzeichnis für technische und semantische Standards, Profile und Leitfäden im Gesundheitswesen aufzubauen, zu pflegen und zu betreiben (§ 291e Abs. 1 SGB V). Die gematik bedient sich hierzu verschiedener Experten aus dem Bereich der Gesundheitsversorgung und der Informationstechnik.[105] Das Verzeichnis wurde fristgerecht online gestellt und lässt sich über https://www.vesta-gematik.de/[106] abrufen. Hierüber können Akteure aus dem Bereich der Informations- und Kommunikationstechnologie im Gesundheitswesen nunmehr Anträge auf Aufnahme eines IT-Standards in das Interoperabilitätsverzeichnis stellen.

---

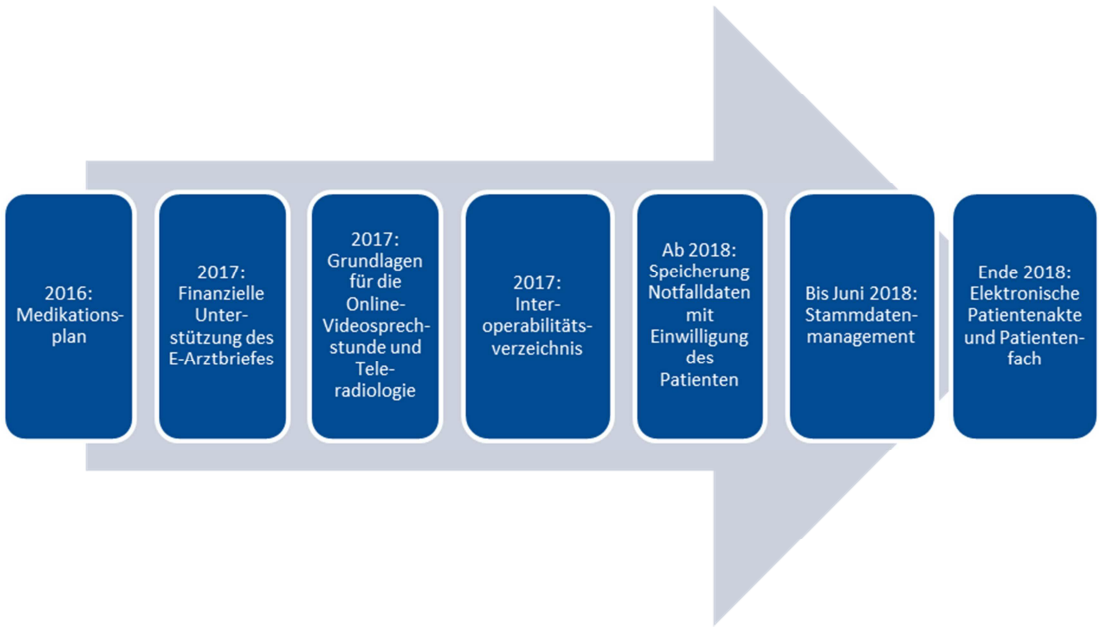
[101] Pressemitteilung der gematik v. 02.06.2017, https://www.gematik.de/cms/de/header_navigation/presse/meldungen_1/Pressemitteilungen.jsp (zuletzt abgerufen am 03.08.2017).
[102] Di Bella, RDG 2015, 90, 91.
[103] Gematik, 2. Statusbericht der Gematik 2016, S. 25.
[104] Deutscher Industrie- und Handelskammertag, Stellungnahme zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, S. 1, abrufbar unter: http://www.dihk.de/themenfelder/wirtschaftspolitik/fachkraeftesicherung-verantwortung/gesundheitswirtschaft/positionen/e-health-gesetz (zuletzt abgerufen am 02.08.2017).
[105] Paland/Holland, NZS 2016, 247, 254.
[106] Zuletzt abgerufen am 08.08.2017.

Interoperabilität in der Praxis

Zusammen mit weiteren Beteiligten hat die Arbeitsgemeinschaft Interoperabilität des Bundesverbandes Gesundheits-IT[107] ein Interoperabilitätsforum entwickelt, in welchem Leitfäden zu spezifischen Praxisproblemen kostenlos eingesehen werden können. Dieses ist unter: wiki.hl7.de/ abrufbar.[108]

Die geplante zeitliche Abfolge der erwähnten E-Health-Anwendungen lässt sich durch nachfolgende Abbildung veranschaulichen:

Abbildung 7
Zeitabfolge nach dem E-Health-Gesetz



[107] Der Bundesverband Gesundheits-IT (bvitg e.V.) vertritt Deutschlands führende IT-Anbieter im Gesundheitswesen, weitere Informationen sind unter http://www.bvitg.de/ abrufbar (zuletzt abgerufen am 02.08.2017).
[108] Zuletzt abgerufen am 02.08.2017.

3.3 Was fehlt? Desiderate im E-Health-Recht

Die Vorgaben des neuen E-Health-Gesetzes werden überwiegend positiv bewertet, sie können aber nur den ersten Schritt auf dem Weg zum digitalisierten Gesundheitswesen darstellen.[109] In der Fachliteratur besonders hervorgehoben werden häufig die im Gesetz enthaltenen Bestimmungen zum Datenschutz. Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein bezeichnet diese sogar als vorbildlich.[110] Jedoch muss mittels Erhöhung der Kontrolldichte und -intensität von Informationsdienstleistern im Medizinbereich sichergestellt werden, dass bestehende Vorgaben auch dauerhaft eingehalten werden. Darüber hinaus dürfen wirtschaftliche Veränderungen bei den beteiligten Leistungserbringern wie z.B. Fusionen oder Betriebswechsel nicht dazu führen, dass datenschutzrechtliche Vorgaben ausgehöhlt werden können, wozu noch weitere rechtliche Bestimmungen erforderlich sind.

Kritisiert wird ebenfalls, dass allein die Schaffung finanzieller Anreize, wie z.B. beim elektronischen Arztbrief, bzw. die Androhung von Sanktionen, etwa bei Nichteinhaltung vorgesehener Fristen, keinesfalls ausreichend sein kann, um die Digitalisierung im Gesundheitswesen normativ zu etablieren.[111] Im Bereich der Interoperabilität wird bemängelt, dass das Gesetz noch keine ausreichenden und transparenten Vorgaben macht, gerade die Industrie aber eben solche benötigt, um die Vorgaben umsetzen zu können.[112] Transparenz ist dabei aber ein maßgeblicher Faktor, um die Interoperabilität der IT-Systeme gewährleisten zu können.[113] Wie bereits zu Beginn festgestellt, ist die rechtliche Umsetzung der Digitalisierung nicht alleine durch das E-Health-Gesetz getan, vielmehr ist dieses nur ein erster Schritt auf einem langen Weg. Aktuelle Themen, wie z.B. Big Data im Gesundheitswesen, effektiver Patientenschutz oder die angemessene Beteiligung der Patienten bei der Gesundheitsversorgung bleiben im Gesetz unerwähnt.

---

[109] So statt vieler Starnecker/Kuhls, jurisPR-ITR 20/2015, Anm. 2; Buchner, MedR 2016, 660, 664; Deutsches Ärzteblatt 2015, Heft 17, S. 761; ehealth-Gesetz: Das sagen Kritiker, abrufbar unter: https://ehealthblog.de/2016/03/06/ehealth-gesetz-das-sagen-kritiker/ (zuletzt abgerufen am 02.08.2017); Bergmann, MedR 2016, 497, 498.

[110] ULD-Stellungnahme zum Referentenentwurf für ein E-Health-Gesetz, S. 3, https://www.datenschutzzentrum.de/artikel/874-ULD-Stellungnahme-zum-Referentenentwurf-fuer-ein-E-Health-Gesetz.html (zuletzt abgerufen am 08.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

[111] Bundesverband Verbraucherzentrale, Stellungnahme zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, S. 11.

[112] Bitkom, E-Health-Gesetz: Bundestag schafft Grundlage für bessere medizinische Versorgung, https://www.bitkom.org/Presse/Presseinformation/E-Health-Gesetz-Bundestag-schafft-Grundlage-fuer-bessere-medizinische-Versorgung.html (zuletzt abgerufen am 02.08.2017).

[113] Bundesverband Gesundheits-IT, Stellungnahme zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, 12.06.2015, S. 2, http://www.bvitg.de/positionspapiere.html (zuletzt abgerufen am 02.08.2017).

Bestehende Regelungslücken lassen sich in folgenden Bereichen ausmachen:[114]

- Es mangelt an Vorgaben für medizinische Anwendungen, die noch nicht durch das E-Health-Gesetz erfasst sind.

- Der Bereich der Telemedizin muss sowohl im SGB V, in den Krankenhausgesetzen als auch in den Musterberufsordnungen konkret und rechtssicher geregelt werden.

- Es müssen die Voraussetzungen für die Etablierung und Weiterentwicklung lokaler IT-Systeme bei den Leistungserbringern geschaffen werden.

- Es fehlt an einer verbindlichen Qualitätskontrolle im Bereich der mobilen Apps, Internetportale und weiterer digitaler Gesundheitsprodukte.

- Es müssen zudem verbindliche Standards definiert und eine Verpflichtung eingeführt werden, Schnittstellen offenzulegen.

- Die Entwicklung sektorübergreifender Lösungen muss vorangetrieben werden.

Auch die Verarbeitung von Gesundheitsdaten in Ländern wie z.B. den USA ist derzeit nicht ausreichend reguliert.[115]
Weiterer Regelungsbedarf besteht zudem im Bereich der Telemedizin. Das Verbot der Fernbehandlung, wie es § 7 Abs. 4 der Musterberufsordnung für Ärzte vorsieht, ist mit dem aktuellen Stand der Technik nicht mehr vereinbar und sollte dringend reformiert werden.[116] Die Beschränkung telemedizinischer Angebote auf rein beratende Tätigkeiten verkennt das Potential, das mit diesen einhergeht. Insbesondere in bevölkerungsarmen Gegenden kann mittels der Telemedizin eine qualitativ hochwertige Versorgung der Patienten sichergestellt werden.[117]

Der Gesetzgeber hat den Bereich der Telemedizin durch das E-Health-Gesetz nur am Rande behandelt; es verbleiben insbesondere im Bereich der Fernbehandlung noch erhebliche Rechtsunsicherheiten. Um dem entgegenzuwirken, ist § 7 Abs. 4 der Musterberufsordnung der Ärzte dahingehend zu konkretisieren, dass telemedizinische Maßnahmen jedenfalls zur Behandlung herangezogen werden können.[118] Die Be-

---

[114] Nach der 88. Konferenz der Ministerinnen und Minister, Senatorinnen und Senatoren für Gesundheit der Länder v. 24.-25.06.2015 in Bad Dürkheim, https://www.gmkonline.de/documents/Ergbnisniederschrift_extern.pdf (zuletzt abgerufen am 02.08.2017).
[115] Dazu näher unter 4.3.3.3.
[116] Deutsche Gesellschaft für Telemedizin, KTM 4/2015, S. 62.
[117] Verbraucherzentrale Bundesverband, Mehr Autonomie wagen – Qualität, Datenschutz und Solidarsystem sicher stellen, S. 7, http://www.vzbv.de/sites/default/files/16-10-17_vzbv_forderungspapier_digitale_gesundheitsversorgung.pdf (zuletzt abgerufen am 02.08.2017).
[118] Bergmann, MedR 2016, 497, 506.

schränkung auf rein diagnostische Anwendungen (Sprechstunde/Röntgenbilder) ist mit dem heutigen Verständnis von Digitalisierung im Gesundheitswesen nicht mehr vereinbar. Therapeutische und pflegerische Maßnahmen müssen ebenfalls im Bereich der Telemedizin möglich sein.[119]

Desiderate finden sich ebenfalls bei der Einbindung des Patienten in das digitale Gesundheitswesen. Zur effektiven Einbindung des Patienten sind die folgenden Maßnahmen zu treffen:[120]

- bessere patientenorientierte Koordination der Versorgungsstrukturen
- umfassende Einsichtsrechte in therapierelevante Daten für Arzt und Patient gleichermaßen
- aktive Einbeziehung der Patienten in Behandlung und Forschung
- Transparenz im Gesundheitswesen und verständliche Informationen
- Förderung des digital kompetenten Patienten

Beispiel 1: Rechtsunsicherheit bei Big Data im Gesundheitswesen

---

Gerade mit Blick auf die groß angelegte Analyse von Gesundheitsdaten (Stichwort: Big Data[121]) zu Forschungs- und/oder Wirtschaftlichkeitszwecken ist es Aufgabe des Gesetzgebers, einen gesetzlichen Rahmen zu schaffen, welcher allen beteiligten Akteuren ausreichend Orientierungssicherheit bietet.[122] Das derzeitige Datenschutzrecht setzt hohe Anforderungen an die Zulässigkeit von Big Data-Analysen im Gesundheitsbereich, insbesondere hinsichtlich möglicher gesetzlicher Erlaubnisnormen. Nicht unberücksichtigt bleiben darf dabei jedoch stets das verfassungsrechtlich geschützte[123] informationelle Selbstbestimmungsrecht der Patienten (vgl. die Ausführungen im Einzelnen unter 4.4).

---

[119] Deutscher Industrie- und Handelskammertag, Stellungnahme zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, S. 6, http://www.dihk.de/themenfelder/wirtschaftspolitik/fachkraeftesicherung-verantwortung/gesundheitswirtschaft/positionen/e-health-gesetz (zuletzt abgerufen am 02.08.2017).
[120] Nach: Verbraucherzentrale Bundesverband, Mehr Autonomie wagen – Qualität, Datenschutz und Solidarsystem sicher stellen, S. 6, http://www.vzbv.de/sites/default/files/16-10-17_vzbv_forderungspapier_digitale_gesundheitsversorgung.pdf (zuletzt abgerufen am 02.08.2017).
[121] Vgl. zum Begriff Hackenberg, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 44. EL 2017, Teil 16.7 Rn. 1 ff.
[122] Vgl. zu Big Data-Verfahren im Allgemeinen bereits die vbw Studie „Big Data im Freistaat Bayern – Chancen und Herausforderungen“, 2016, S. 126 ff.
[123] Hierzu bereits unter 3.1.2.

Beispiel 2: Rechtsunsicherheit bei Gesundheits-Apps

Auch der Bereich Mobile Health (mHealth), ein Teilbereich des E-Health,[124] ist bislang nur ungenügend reguliert und von den Vorgaben des E-Health-Gesetzes nicht erfasst. Dabei können mHealth-Dienste von entscheidender Bedeutung sein, um weiterhin ein leistungsfähiges Gesundheitswesen zu ermöglichen.[125] In der Praxis bieten sich zahlreiche Anwendungsbereiche an, die von simplen Erinnerungsfunktionen bezüglich der Medikamenteneinnahme bis hin zu telemedizinischen Anwendungen reichen.[126] Weiterhin lässt sich eine Verknüpfung zum Themenkomplex Big Data herstellen, nachdem die durch die Apps gewonnenen Daten ihrerseits wiederum im Grundsatz für Analysen verwendet werden können. Der flächendeckenden Nutzung und Integration von Mobile-Health-Diensten im Gesundheitswesen steht allerdings der Umstand entgegen, dass diese bislang nicht im Verzeichnis der abrechnungsfähigen Leistungen aufgenommen sind und somit nicht in die Regelversorgung der gesetzlichen Krankenkassen fallen.[127] Bei der Entwicklung und Anwendung sind hingegen zahlreiche Vorgaben aus dem Medizinprodukterecht, dem Datenschutzrecht sowie dem allgemeinen Haftungsrecht zu beachten.[128]

Es bleibt festzuhalten, dass im Bereich der Mobile-Health-Dienste einerseits eine Vielzahl von Bestimmungen berührt wird, andererseits aber klare Leitlinien oder Zulassungsvoraussetzungen durch den Gesetzgeber fehlen.[129] In der Antwort der Bundesregierung vom 07.11.2016 auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN stellte die Bundesregierung durch einen Verweis auf die ab Mai 2018 geltende EU-Datenschutzgrundverordnung (EU-DSGVO) allerdings auch klar, dass der internationale App-Markt insbesondere datenschutzrechtlich nicht abschließend durch nationale Regelungen bestimmt werden könne.[130] Das Bundesministerium für Gesundheit begleite jedoch die Ausarbeitung einer Selbstverpflichtung der Hersteller von Gesundheits-Apps in Bezug auf Qualität und Datenschutz als Verhaltensregel i.S.d. Art. 40 EU-DSGVO.

Einen ersten Schritt in Richtung „Mehr Rechtssicherheit“ hat der Gesetzgeber kürzlich mit der Verabschiedung von gesetzlichen Neuregelungen zur Einschaltung externer Dienstleister durch Berufsgeheimnisträger wie z.B. Ärzte, Apotheker und Rechtsanwäl-

[124] Vgl. dazu World Health Organization, mHealth, S. 6, http://www.who.int/reproductivehealth/publications/mhealth/en/ (zuletzt abgerufen am 02.08.2017).
[125] Grünbuch über Mobile-Health-Dienste (mHealth) v. 10.04.2014, KOM(2014) 219 endg., S. 15.
[126] Zu den möglichen Anwendungsbereichen: World Health Organization, mHealth, S. 19 ff.
[127] Rübsamen, MedR 2015, 485, 490.
[128] Rübsamen, MedR 2015, 485, 486. Vgl. im Einzelnen unter 4.3.
[129] Jandt/Hohmann, Life-Style-, Fitness- und Gesundheits-Apps, in: Taeger (Hrsg.), Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft, Tagungsband DSRI-Herbstakademie 2015, S. 30.
[130] BT-Drs. 18/10259, S. 4. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.

te unternommen. Der entsprechende Gesetzentwurf[131] wurde am 01.07.2017 vom Bundestag beschlossen. Die neuen Bestimmungen sind jedoch noch nicht in Kraft, nachdem die Verkündung im Bundesgesetzblatt derzeit[132] noch aussteht. Hintergrund ist, dass nicht nur im Gesundheitsbereich die Leistungserbringer bei der Nutzung moderner Informationstechniken auf die Unterstützung von Drittanbietern angewiesen sind, zugleich damit allerdings bisher stets die Gefahr eines Verstoßes gegen § 203 StGB verbunden ist.[133] In § 203 Abs. 3 Satz 2 StGB n.F. wird nunmehr geregelt, dass keine unbefugte Offenbarung eines fremden Geheimnisses für den Fall anzunehmen ist, in dem dies gegenüber dritten Personen geschieht, die an der beruflichen Tätigkeit des Arztes, Rechtsanwalts etc. mitwirken und eine solche Offenbarung auch für die Inanspruchnahme der externen Dienstleister *erforderlich* ist. Wichtig ist jedoch, dass der Berufsgeheimnisträger dafür Sorge zu tragen hat, externe Dienstleister über die Geheimhaltungspflicht zu belehren, um selbst keiner strafrechtlichen Verantwortlichkeit zu unterliegen (vgl. § 203 Abs. 4 Satz 2 Nr. 1 SGB n.F.). Im Gegenzug werden die Dienstleister selbst in eine mögliche Strafbarkeit nach § 203 StGB einbezogen, damit durch die gelockerten Bestimmungen insgesamt kein niedrigeres Schutzniveau für die Daten von Mandanten und Patienten entsteht. Die Gesetzesreform ist zu begrüßen, nachdem insbesondere der Einsatz externer Dienstleister etwa für die Abrechnung auch im Gesundheitswesen immer mehr an Bedeutung gewinnt.[134] Dies gerade vor dem Hintergrund, dass – wie bereits erwähnt – die Nutzung von IT-gestützten Prozessen ausdrücklich durch das E-Health-Gesetz gefördert und gefordert wird.[135]

3.4 Übergeordnete Handlungsmaximen für ein digitalisiertes Gesundheitswesen

Allgemeine Grundsätze, darunter insbesondere solche aus dem Bereich des Datenschutzes sowie Handlungsempfehlungen auf europäischer und nationaler Ebene tragen entscheidend zur Rechtssicherheit bei. Sowohl bei der Planung als auch bei der letztlichen Beurteilung konkreter digitaler Anwendungen im Gesundheitswesen sind diese Vorgaben zu berücksichtigen. Insbesondere bei Vorgängen, die noch keinen konkreten Niederschlag im Gesetz gefunden haben, kann eine erste *Vorabkontrolle* anhand dieser Richtlinien erstellt werden. So kann z.B. eine Anwendung, die ohne Einwilligung oder gesetzlichen Erlaubnistatbestand Daten erhebt, nicht zulässig sein. Andererseits bedarf es unter Umständen keiner Rechtfertigung für die Datenverarbeitung, wenn diese anonymisiert erfolgt.

---

[131] Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, BT-Drs. 18/11936.
[132] Stand: 08.08.2017.
[133] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), Entschließung der 89. Datenschutzkonferenz, https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Datenschutz/DSK/Entschliessungen/089_ehealth.html (zuletzt abgerufen am 02.08.2017).
[134] Spindler, MedR 2016, 691, 696.
[135] Weichert, IGZ Nr. 2/2015, S. 29.

3.4.1 Datenschutzrechtliche Grundsätze

Neben dem konkreten Nutzen für den Patienten ist bei der Digitalisierung des Gesundheitswesens stets der Schutz seiner Daten zu berücksichtigen. Kerngedanke des Datenschutzes ist es, die informationelle Selbstbestimmung des Einzelnen zu wahren; grundsätzlich soll allein der Betroffene über den Umgang mit seinen Daten entscheiden.[136]

Bei jeder Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind die folgenden Grundsätze zu beachten:

- Das Verbot mit Erlaubnisvorbehalt besagt, dass jeder Umgang mit personenbezogenen Daten grundsätzlich verboten ist, sofern der Betroffene nicht eingewilligt hat oder ein gesetzlicher Erlaubnistatbestand vorliegt.[137]

- Datenschutz als Persönlichkeitsschutz gilt nur für personenbezogene Daten. Das sind nach der Definition in § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Bei Einzelangaben wiederum handelt es sich um Informationen, welche sich auf eine bestimmte natürliche Person beziehen, oder auch nur um solche, die geeignet sind, einen Bezug zu eben dieser Person herzustellen.[138] Die EU-DSGVO spricht – in inhaltlicher Übereinstimmung mit dem bisherigen nationalen Recht[139] – von „Informationen über identifizierte oder identifizierbare natürliche Personen“ (Art. 4 Nr. 1).

- Der Zweckbindungsgrundsatz verlangt, dass die Verarbeitung personenbezogener Daten auf Grundlage eines bestimmten Zwecks erfolgen muss.[140] Dieser ist von der datenverarbeitenden Stelle bereits vor der Verarbeitung festzulegen und sollte daher vorzugsweise dokumentiert werden.[141] Will die datenverarbeitende Stelle die Daten zu einem anderen als dem ursprünglich vereinbarten Zweck verarbeiten, benötigt sie die erneute Einwilligung des Betroffenen.[142]

---

[136] Ausführlich dazu Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 23 ff.
[137] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4 Rn. 3; Schantz, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 5 EU-DSGVO Rn. 5.
[138] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 11 TMG Rn. 6.
[139] Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 3.
[140] Helfrich, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 44. EL 2017, Teil 16.1 Rn. 80; Schantz, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 5 EU-DSGVO Rn. 13 ff.
[141] Helfrich, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 44. EL 2017, Teil 16.1 Rn. 81; Schantz, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 5 EU-DSGVO Rn. 14.
[142] Seiler, jurisPR-BKR 3/2012, Anm. 5; Schantz, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 5 EU-DSGVO Rn. 22.

- Den Erforderlichkeitsgrundsatz hat der Gesetzgeber gleich an mehreren Stellen im Datenschutzregime des SGB und BDSG sowie auch der EU-DSGVO festgeschrieben. Erforderlichkeit ist nur dann gegeben, wenn der beabsichtigte Umgang mit den personenbezogenen Daten das zur Zweckerreichung mildeste Mittel darstellt.[143] Es darf demnach kein anderes Mittel zur Verfügung stehen, mit welchem dieser Zweck genauso gut erreicht werden könnte und das weniger stark in die Rechte des Betroffenen eingreift.

- Der Transparenzgrundsatz verlangt, dass der Betroffene weiß, welche Daten über ihn erhoben werden.[144] Der Betroffene muss die Information haben, welche seiner Daten zu welchem Zweck bei welcher Stelle für wie lange und aus welchem Grund gespeichert werden.[145] Ferner ist wichtig, dass für ihn die Risiken der Verarbeitung auch schon im Voraus erkennbar sind.[146]

- Im Rahmen informationeller Gewaltenteilung wird der Zweckbindungsgedanke auf eine einzelne datenverarbeitende Stelle, die unterschiedliche Aufgaben wahrnimmt, übertragen.[147] Hier ist eine organisatorische Trennung in der Form erforderlich, dass ein Informationsaustausch verhindert wird.

- Von besonderer Bedeutung ist nicht zuletzt der Grundsatz der Datenvermeidung bzw. Datensparsamkeit. Seine gesetzliche Entsprechung findet sich in § 3a BDSG. Auf Ebene der ab März 2018 geltenden EU-DSGVO sind in diesem Zusammenhang im Wesentlichen zwei Artikel von Relevanz: einerseits der Grundsatz der Datenminimierung in Art. 5 Abs. 1 lit. c EU-DSGVO und andererseits die gesonderten Bestimmungen zum Datenschutz durch Technikgestaltung (Privacy by design) und durch datenschutzfreundliche Voreinstellungen (Privacy by default) in Art. 25 EU-DSGVO. Zu erwähnen sind in diesem Zusammenhang insbesondere die Anonymisierung und die Pseudonymisierung.

  Für die Anonymisierung (im Sinne des § 3 Abs. 6 BDSG) ist es notwendig, dass die Daten dergestalt verändert werden, dass ein Personenbezug nicht oder nur mit einem unverhältnismäßig hohen Aufwand hergestellt werden kann. Konsequenz der Anonymisierung ist, dass das Datenschutzrecht auf solche Daten nicht mehr anwendbar ist.[148] Gerade in datenschutzrechtlich bedenklichen Fällen bietet sich dieses Verfahren an, da das Nichtvorliegen

---

[143] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 14 f.; Albers, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, Art. 6 EU-DSGVO Rn. 17.
[144] Brandt, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 29 Rn. 19.
[145] Härting, CR 2011, 169, 170.
[146] Schantz, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 5 EU-DSGVO Rn. 11.
[147] Polenz, in: Kilian/Heussen, Computerrechts-Handbuch, 33. EL 2017, Teil 13 II. Rn. 9; Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 6 Rn. 25 m.w.N.
[148] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3a Rn. 9.

personenbezogener Daten im Gegenzug auch die Nichtbeachtung vorgenannter Grundsätze legalisiert. Zu beachten ist allerdings, dass es für eine Anonymisierung nicht ausreichend ist, die Einzelangaben einer Person zu löschen.[149] Die Wiederherstellung des Personenbezugs (*Reanonymisierung*), wie es z.B. durch verbleibende anderweitige Merkmale möglich sein kann, muss ausgeschlossen sein.[150] Um dies zu erreichen, wird eine Datenaggregierung vorgeschlagen.[151] Erhobene Daten werden dabei in derart großen einheitlichen Gruppen zusammengefasst, dass eine Bestimmung einzelner Merkmale der Ursprungsdatensätze nicht mehr möglich ist.[152]

Die Legaldefinition der Pseudonymisierung findet sich in § 3 Abs. 6a BDSG bzw. Art. 4 Nr. 5 EU-DSGVO. Demnach sind für die Pseudonymisierung die Identifikationsmerkmale der betroffenen Person durch Kennzeichen zu ersetzen, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. In der Folge kommen die strengen Regelungen des Datenschutzrechts jedenfalls dann ebenfalls nicht zur Anwendung, wenn die betreffende Stelle nicht auf die Zuordnungsfunktion zugreifen kann und Aufdeckungsrisiken auf ein hinzunehmendes Maß reduziert sind.[153] Anderenfalls sind die datenschutzrechtlichen Vorgaben aufgrund des weiterhin vorhandenen Personenbezugs zwar noch immer anwendbar, jedoch kann ggf. auf besondere Schutzvorkehrungen hinsichtlich des Zugangs oder Zugriffs auf pseudonymisierte Daten verzichtet werden.[154]

Weiterhin stellt sich die noch nicht abschließend geklärte Frage, ob die datenschutzrechtlich verantwortliche Stelle eine (erneute) Einwilligung des Betroffenen in die Anonymisierung bzw. Pseudonymisierung seiner Daten einholen muss, wofür gerade im Kontext der Verarbeitung von Gesundheitsdaten (vgl. Art. 4 Nr. 15 EU-DSGVO) – zumindest vorsorglich – die besseren Gründe sprechen.[155]

---

[149] Roßnagel, ZD 2013, 562, 565.
[150] Schefzig, Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen, in: Taeger (Hrsg.), BIG DATA & CO. – Neue Herausforderungen für das Informationsrecht, Tagungsband DSRI-Herbstakademie 2014, S. 113.
[151] Weichert, ZD 2013, 251, 259.
[152] Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 4 Rn. 49.

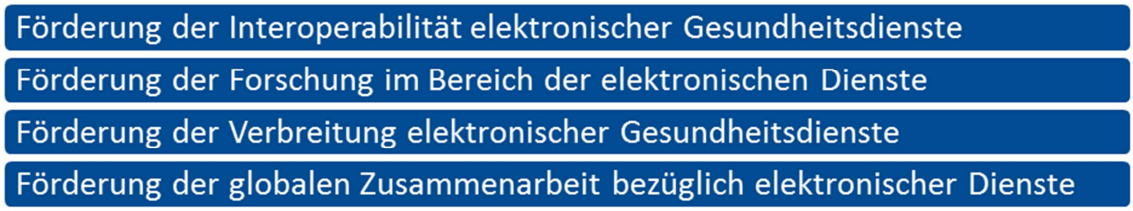
[154] Schild, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, Art. 4 EU-DSGVO Rn. 78.
[155] Vgl. hierzu bereits die vbw Studie „Big Data im Freistaat Bayern – Chancen und Herausforderungen“, 2016, S. 108 f.

3.4.2 Europäische Vorgaben

Die Europäische Union hat sich die Verbesserung der Gesundheit der Bürger unter Einsatz elektronischer Gesundheitsdienste zum Ziel gesetzt. Primärrechtliche Grundlagen finden sich z.B. in den Vorgaben zur Waren- und Verkehrsdienstleistungsfreiheit gem. Art. 34 und 56 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV).

Angestrebt wird dabei konkret die Erhöhung von Qualität und Zugänglichkeit der medizinischen Versorgung durch effiziente, benutzerfreundliche und umfassend akzeptierte elektronische Gesundheitsdienste.[156] E-Health soll dabei durch die Verbesserung der Interoperabilität neuer Technologien im digitalen Binnenmarkt gefördert werden, die Bürger und Unternehmen gleichermaßen inkludieren.[157] Mit dem Aktionsplan für elektronische Gesundheitsdienste 2012-2020[158] wird zur engen Zusammenarbeit zwischen nationalen und regionalen Behörden, Angehörigen der Gesundheits- und Sozialberufe, Industrie, Patienten, Dienstleister, Wissenschaftler und EU-Organen aufgerufen, um die folgenden Ziele innerhalb der EU zu verwirklichen:

Abbildung 8
Europäische Zielsetzungen im E-Health-Bereich



3.4.3 Nationale Strategien zur Digitalisierung im Gesundheitswesen

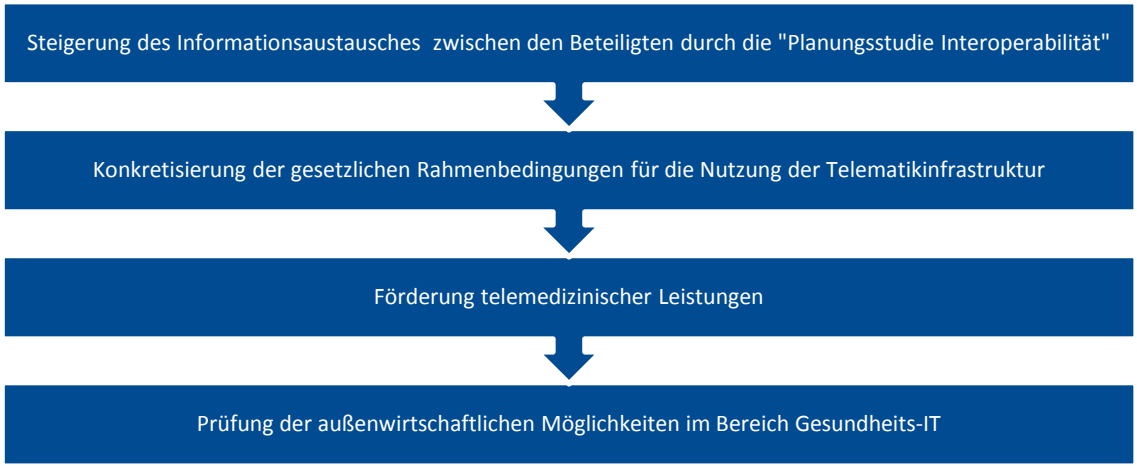
Auch auf nationaler Ebene finden sich zahlreiche Initiativen, die die Digitalisierung im Gesundheitswesen vorantreiben sollen. Sowohl die einzelnen Länder als auch die Bundesregierung haben Strategien für den Ausbau der elektronischen Gesundheitsdienste erarbeitet. Auf Landesebene sei hier beispielsweise die Digitalstrategie des Landes Hessen genannt, die im Bereich des Gesundheitswesens insbesondere digitale Technologien fördern möchte, um z.B. die Patientensicherheit und Qualitätssicherung

[156] Ziele der EU im Bereich eGesundheit, http://ec.europa.eu/health/ehealth/policy/index_de.htm (zuletzt abgerufen am 02.08.2017).
[157] Strategien für einen digitalen Binnenmarkt für Europa v. 06.05.2015, KOM (2015) 192 endg., S. 18.
[158] KOM (2012) 736 endg., dort insbesondere S. 7.

zu verbessern.[159] Im Freistaat wird das Thema u. a. von dem Zentrum Digitalisierung.Bayern besetzt, das die Themenplattform Digitale Gesundheit / Medizin betreibt.

Auf Bundesebene gründete das Bundesgesundheitsministerium bereits 2010 die „E-Health-Initiative“, die die Einführung telemedizinischer Anwendungen begünstigen soll, indem entgegenstehende Hürden identifiziert und (möglichst) beseitigt werden.[160] Im September 2015 veröffentlichte die Bundesregierung die „Strategie Intelligente Vernetzung“, die vier konkrete Maßnahmen nennt, um das Gesundheitswesen durch die digitale Kommunikation leistungsfähiger zu gestalten:[161]

Abbildung 9
Zielsetzungen der Bundesregierung im E-Health-Bereich



[159] Abrufbar unter https://www.digitalstrategie-hessen.de/img/Digitalstrategie_Hessen_2016_ver1.pdf, S .88 (zuletzt abgerufen am 02.08.2017).
[160] Bundesministerium für Gesundheit, E-Health-Initiative und Telemedizin, https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-initiative-und-telemedizin/e-health-initiative.html (zuletzt abgerufen am 02.08.2017).
[161] Abrufbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/Intelligente-Vernetzung/strategie-intelligente-vernetzung.html, S. 15 (zuletzt abgerufen am 02.08.2017).

Festzuhalten bleibt, dass das digitale Gesundheitswesen von allen Beteiligten gewünscht wird, die rechtlichen Vorgaben dem technisch Möglichen allerdings (noch) nicht gerecht werden. Das E-Health-Gesetz ist – ebenso wie die Datenschutz–Grundverordnung auf europäischer Ebene – der richtige Weg, den der Gesetzgeber nunmehr konsequent weiter beschreiten sollte, damit das Recht nicht zum digitalen Stolperstein des gesundheitlichen Fortschritts wird.

4 Ausgewählte Problemfelder

Vernetzung, Datenschutz und Big Data

Neben der Vernetzung im Gesundheitswesen im Allgemeinen spielt die datenschutzkonforme Einwilligung in die Verarbeitung von Gesundheitsdaten im Speziellen eine große Rolle, was eine nähere Beleuchtung beider Themenkomplexe rechtfertigt. Ein Rechtskonformitäts-Check für Gesundheits-Apps soll die Praxis für einige wichtige rechtliche Stolpersteine sensibilisieren. Abschließend werden Big Data-Analysen von Gesundheitsdaten aus juristischer Sicht betrachtet.

4.1 Rechtliche Herausforderungen für die Vernetzung im Gesundheitswesen

4.1.1 Allgemeine Herausforderungen

Trotz aller bisherigen Bemühungen sind die einzelnen Akteure im Gesundheitswesen (Patienten, Leistungserbringer, Leistungsträger) untereinander noch zu wenig vernetzt. An den „Schnittstellen“ im Bereich der gesundheitlichen Versorgung wird die fehlende Vernetzung besonders deutlich.[162] Ein Beispiel hierfür ist der Übergang zwischen stationärer und ambulanter Behandlung im Krankenhaus.[163] Nicht ohne Probleme läuft auch der patientenbezogene digitale Datenaustausch ab.[164]

Kompatibilitätsdefizite liegen daran, dass die einzelnen Akteure unterschiedliche IT-Infrastrukturen nutzen. Oft wird sogar innerhalb einer Einheit, z.B. einem Krankenhaus, mit untereinander nicht kompatiblen IT-Systemen gearbeitet. Daher müssen Patientendaten in aller Regel immer noch auf Papier übermittelt werden.

Der Gesetzgeber hat dieses Problem erkannt und versucht, diesem mit dem E-Health-Gesetz und der damit verbundenen Einführung der elektronischen Gesundheitskarte beizukommen. Die Akteure im Gesundheitswesen stehen dabei vor enormen rechtlichen und tatsächlichen Herausforderungen. Neben den neuen spezialgesetzlichen Regelungen im E-Health-Gesetz gelten im vernetzten Gesundheitswesen selbstverständlich weiterhin die allgemeinen (datenschutz-)gesetzlichen und untergesetzlichen Vorgaben wie sie für das Offline-Gesundheitswesen bestehen: Die Vernetzung darf

---

[162] Paland/Holland, NZS 2016, 247.
[163] Schröder-Printzen, in: Tebille/Clausen/Schroeder-Printzen, Münchener Anwaltshandbuch Medizinrecht, 2. Aufl. 2013, § 10 Rn. 1.
[164] Wehrmann/Wellbrock, CR 1997, 754, 759.

nicht unverhältnismäßig in das Grundrecht auf informationelle Selbstbestimmung eingreifen. Zudem ist zu beachten, dass das Gesetz Gesundheitsdaten als besondere Kategorie von Daten nach § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 EU-DSGVO in besonderem Maße unter Schutz stellt, was den Umgang mit ihnen in der Praxis nicht erleichtert. Im Übrigen befreit die – grundsätzlich begrüßenswerte – Vernetzung Ärzte und andere Berufsgeheimnisträger nicht von ihrer Schweigepflicht (§ 203 StGB). Erstgenannte müssen schließlich auch im vernetzten Gesundheitswesen ihren Dokumentationspflichten nach § 10 der Musterberufsordnung für Ärzte nachkommen.

Vernetzung bedeutet im Übrigen auch, dass zahlreiche computerspezifische Regelungen wie z.B. jene zum Schriftformersatz (siehe § 126a BGB, § 3a Abs. 2 BayVwVfG, § 36a SGB I) zur Anwendung kommen.

4.1.2 Besondere Herausforderungen im Gesundheitssektor

Das BDSG stellt Gesundheitsdaten als besondere Kategorie personenbezogener Daten nach § 3 Abs. 9 BDSG unter vorrangigen Schutz. Unter Gesundheitsdaten fallen zunächst unmittelbare Angaben über die Gesundheit, mithin sämtliche Daten, die den physischen oder psychischen Zustand einer natürlichen Person betreffen.[165] Zu beachten ist, dass es bei der Frage nach der Sensitivität eines personenbezogenen Datums exklusiv auf dessen Verwendungskontext ankommt.[166] Ein Datum ist folglich bereits dann als Gesundheitsdatum einzuordnen, wenn es mittelbar aus dem Gesamtzusammenhang oder durch Verknüpfung mit weiteren Daten einen Rückschluss auf ein sensitives Datum zulässt.[167] Daher können Informationen über einzelne Krankenhaus-/Arztbesuche, Krankheiten oder medizinische Behandlungen einschließlich der eingenommenen Medikamente ebenso wie die Feststellung, dass eine Person mittlerweile wieder genesen/gesund ist, Gesundheitsdaten darstellen.[168] Als besondere Kategorie personenbezogener Daten räumt das Gesetz Gesundheitsdaten einen gegenüber sonstigen personenbezogenen Daten erhöhten Schutz ein, denn der Verwendungszusammenhang von Gesundheitsdaten legt deren Sensitivität nahe.[169]

Das BDSG normiert für Gesundheitsdaten strengere Anforderungen an die Einwilligung und enthält spezielle Erlaubnistatbestände. Die Einwilligung muss sich nach § 4a Abs. 3 BDSG ausdrücklich auf die Erhebung, Verarbeitung oder Nutzung der Gesundheitsdaten beziehen.[170] Die Erlaubnistatbestände für den Umgang mit Gesundheitsdaten orientieren sich entweder an der relevanten Berufsgruppe (vgl. § 28 Abs. 7 BDSG,

---

[165] Art. 29 Datenschutzgruppe; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 56a.
[166] Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 251.
[167] Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 265.
[168] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 56.
[169] Jandt/Hohmann, K&R 2015, 694, 697.
[170] Hierzu ausführlich unter 4.2.

§ 27 BayKHG) oder gehen von einem Vorrang der datenschutzrechtlichen Einwilligung aus. Die spezialgesetzlichen Erlaubnistatbestände verdrängen jene aus dem allgemeinen Datenschutzrecht, sodass ein Rückgriff auf letztere zum Umgang mit Gesundheitsdaten nicht möglich ist.[171] Die Akteure im digitalisierten Gesundheitswesen dürfte immerhin freuen, dass der Umgang mit Gesundheitsdaten grundsätzlich keine zusätzlichen technisch-organisatorischen Maßnahmen als die nach der Anlage zu § 9 BDSG erfordert. Allerdings ist im Rahmen der vorzunehmenden Abwägung durchaus zu berücksichtigen, dass es sich um besonders sensible Daten handelt, was auch auf die Wahl der einzelnen Maßnahmen durchschlagen kann.[172] Zudem sollte der Datenverarbeiter daran denken, dass § 42a Nr. 2 BDSG zur Information gegenüber der zuständigen Stelle und dem Betroffenen verpflichtet, wenn dessen personenbezogene Daten, die einem Berufsgeheimnis (Arzt etc.) unterfallen, einem Dritten widerrechtlich zur Kenntnis gelangen.

Im Gesundheitswesen bestehen einerseits mit dem 10. Kapitel des SGB V und andererseits mit den Landeskrankenhausgesetzen (in Bayern: § 27 BayKHG; in Hessen: § 12 HKHG; etc.) spezifische – oft sehr restriktive – Datenschutzregelungen. Das Bundessozialgericht ist zudem der Ansicht, dass im Geltungsbereich des SGB V die Verwendung von Patientendaten ausschließlich und auch nur in dem Umfang erlaubt ist, in dem die vorhandenen bereichsspezifischen Vorschriften des SGB V dies gestatten.[173] Die allgemeinen datenschutzrechtlichen Regelungen (des BDSG usw.), die eine Datenübermittlung bei Vorliegen einer Einwilligungserklärung des Betroffenen erlauben, finden daher insoweit grundsätzlich keine Anwendung, es sei denn, das SGB V gestattet die Einwilligung ausdrücklich oder weist insoweit eine Regelungslücke auf. Für Krankenhäuser und Kassenärzte heißt das, dass sie Daten über die gesetzlich krankenversicherten Patienten nicht an private Abrechnungsstellen weitergeben dürfen. Dies gilt sogar dann, wenn der Patient vorher ausdrücklich eingewilligt hat.
Im Gegenzug können auch die gesetzlichen Krankenkassen Datenübermittlungen über ihre Versicherten und die Leistungserbringer nicht über eine Einwilligungserklärung legitimieren.[174] Denn dies sehen die §§ 284 ff. SGB V nicht vor.

---

171 Jandt/Hohmann, K&R 2015, 694, 698.
172 Ernestus, in: Simitis, BDSG, 8. Aufl. 2014, § 9 Rn. 25-33.
173 BSG v. 10.12.2008 - B 6 KA 37/07 mit Anm. Berger, jurisPR-ITR 10/2009, Anm. 5.
174 Jandt/Hohmann, K&R 2015, 694, 697.

Beispiel: Vernetzung von Gesundheitsdaten

Derzeit existieren Überlegungen einiger gesetzlicher Krankenkassen, eine Plattform als übergreifendes Netzwerk für Gesundheitsdaten einzuführen, durch welches verschiedene Beteiligte im Gesundheitswesen vernetzt und angeschlossen werden. Hierüber soll umfassendes Datenmaterial über die einzelnen Patienten verfügbar gemacht werden.

Die Einführung eines solchen Systems ist jedoch aus rechtlicher Sicht kritisch zu bewerten. Zunächst ist im Hinblick auf die durch das E-Health-Gesetz geforderte Interoperabilität zunächst dafür Sorge zu tragen, dass sich ein solches System in die Telematikinfrastruktur einfügen kann.

Auch aus datenschutzrechtlicher Perspektive sind zahlreiche Vorgaben zu berücksichtigen. Allen voran ist zu beachten, dass insbesondere die Leistungsträger bei dem Umgang mit Daten an die gesetzlichen Erlaubnistatbestände aus dem SGB V gebunden sind. Ein Rückgriff auf allgemeine Normen ist dabei – wie bereits dargestellt – nur in Ausnahmefällen möglich. Auch die anlasslose Speicherung von Patientendaten in einem solchen System bereitet mit Blick auf den Zweckbindungs- und Erforderlichkeitsgrundsatz große Probleme. Sofern diese Daten anschließend für Analyse-Zwecke verwendet werden (Stichwort: Big Data), kommt eine datenschutzkonforme Realisierung dieser Vorgänge auf den ersten Blick praktisch nicht mehr in Betracht. Das Wesen einer Big Data-Analyse besteht darin, sehr viele Daten zu sammeln, um diese anschließend für einen anfangs noch nicht genau definierten Zweck zu analysieren. Dieser Umstand steht zu der Vorgabe, dass der Betroffene vor Abgabe seiner Erklärung über den Verwendungszweck seiner Daten Bescheid wissen muss, in eklatantem Widerspruch. Sofern der Betroffene jedoch – zunächst im „bilateralen" Verhältnis zum Anbieter des entsprechenden Dienstes – in verständlicher und transparenter Form über Inhalt, Umfang und Auswirkungen des Dienstes informiert wird und sich diese Aufklärung von Anfang an auch auf weitergehende Datenanalysen bezieht, sind grundsätzlich auch bei der Ausdehnung dieses Verhältnisses auf Big Data-Anwendungen informierte Einwilligungen und mithin auch diesbezügliche Verarbeitungsvorgänge von Gesundheitsdaten rechtskonform denkbar.[175]

Schlussendlich ist ein genaues Augenmerk darauf zu legen, ob die Datenspeicherung im Sinne einer Auftragsdatenverarbeitung der Beteiligten erfolgt oder als echte Funktionsübertragung ausgestaltet wird. Sofern die Initiative eines solchen Netzwerkes durch die Leistungsträger erfolgt, wäre eine Auftragsdatenverarbeitung nach den Vorgaben des § 80 SGB X denkbar.[176] Gem. § 197b SGB V ist es den Leistungsträgern sogar

[175] Vgl. beispielhaft für Gesundheits-Apps die vbw Studie „Big Data im Freistaat Bayern – Chancen und Herausforderungen", 2016, S. 110.
[176] Schneider-Danwitz, in: jurisPK-SGB V, 3. Aufl. 2016, § 197b SGB V Rn. 23.

gestattet, nicht wesentliche Aufgaben an Arbeitsgemeinschaften oder Dritte zu übertragen, sofern dies im wohlverstandenen Interesse des Versicherten liegt und dessen Interessen durch die Einbeziehung nicht beeinträchtigt werden. Höchst fraglich erscheint jedoch, ob die Schaffung eines Sammel-Datenportals über ihre Versicherten zu den gesetzlichen Aufgaben einer Krankenkasse gehört.

Die ab dem 25.05.2018 geltende EU-Datenschutzgrundverordnung enthält eine ausdrückliche Definition der Gesundheitsdaten in Art. 4 Abs. 15 EU-DSGVO, was die herausgehobene Stellung dieser Datenkategorie bereits verdeutlicht. Gesundheitsdaten sind demnach personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Mit Art. 9 EU-DSGVO findet sich auch auf europäischer Ebene eine eigene Vorschrift mit Blick auf die Verarbeitung besonderer Kategorien personenbezogener Daten, welche jedenfalls die Grundstrukturen des bisherigen Rechts beibehält. Zudem enthält die EU-DSGVO in Art. 9 Abs. 4 eine Öffnungsklausel für nationalstaatliche Regelungen, welche sich u.a. auf Gesundheitsdaten bezieht. Auf diese stützen sich die Befürworter der Ansicht, dass auch nach Geltung der EU-Datenschutzgrundverordnung das – soeben dargestellte – sehr detaillierte, bereichsspezifische Sozialdatenschutzrecht in Deutschland weiterhin anwendbar bleibt.[177] Auch das inhaltlich völlig neu gefasste BDSG, welches ebenfalls zum 25.05.2018 in Kraft treten wird, enthält in den §§ 22 ff. BDSG-neu von der EU-Datenschutzgrundverordnung abweichende Rechtfertigungstatbestände. In der rechtswissenschaftlichen Literatur ist jedoch noch umstritten, ob und inwieweit die abweichenden nationalen Vorschriften mit dem Anwendungsvorrang der EU-Verordnung jeweils im Einzelnen in Einklang zu bringen sind. Teilweise wird bereits gefordert, das zunehmend unüberschaubare Regelungsregime des Gesundheitsdatenschutzrechts umfassend zu bereinigen und in einen konsistenteren und transparenteren Regelungsrahmen zu überführen.[178]

4.2 Datenschutzkonforme Einwilligung in die Verarbeitung von Gesundheitsdaten

4.2.1 Ausdrückliche Einwilligung, Kopplungsverbot, zeitliche Entzerrung

Das BDSG normiert für Gesundheitsdaten spezielle Erlaubnistatbestände (vgl. unter 4.1.2) und strengere Anforderungen an die Einwilligung. Diese muss sich nach § 4a

---

[177] Vgl. Buchner/Schwichtenberg, GuP 2016, 218, 223.
[178] Buchner/Schwichtenberg, GuP 2016, 218, 223 f.

Abs. 3 BDSG ausdrücklich auf die Erhebung, Verarbeitung oder Nutzung von Gesundheitsdaten beziehen. Eine Pauschaleinwilligung genügt daher in aller Regel nicht.

Die datenschutzrechtliche Einwilligung ist in Übereinstimmung mit der Terminologie des BGB (vgl. § 183 BGB) stets die vorherige Zustimmung des Betroffenen. Sie zielt darauf ab, einen Eingriff in das (Datenschutz-)Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen.[179] Zur Rechtfertigung des Eingriffs ist mithin die Einwilligungsfähigkeit des Betroffenen Voraussetzung.[180] Nach der Rechtsprechung soll es hierzu ausreichen, wenn der Betroffene die Tragweite der Entscheidung erkennen kann.[181]

Die Einwilligung im Datenschutzrecht verlangt gleichwohl mehr als nur das Fehlen von Willensmängeln; nach § 4a Abs. 1 Satz 1 BDSG muss die Einwilligung auf der freien Entscheidung (Freiwilligkeit) des Betroffenen beruhen. Bereits im Offline-Gesundheitswesen stellt sich häufig die Frage, ob überhaupt noch von einer freien Entscheidung des Betroffenen gesprochen werden kann.[182] Denn eine freie Entscheidung scheidet aus, wenn der Betroffene dadurch zur Abgabe seiner datenschutzrechtlichen Einwilligung bewegt wird, dass ihm bestimmte Leistungen, etwa medizinische Behandlungen, nur dann gewährt werden, wenn er einwilligt (sogenanntes Kopplungsverbot).[183] Man denke dabei nur an Notfallbehandlungen im Krankenhaus. Eine Kopplung von Behandlung und datenschutzrechtlicher Einwilligung verbietet sich hier von vornherein.[184] Zudem dürfte es bereits wegen der vorrangigen Fokussierung auf den pathologischen Zustand an der Freiwilligkeit fehlen.

Das Bundessozialgericht hat bereits 2009 entschieden, dass sich die Kopplungsproblematik auch in medizinisch unterversorgten ländlichen Gebieten oder aber bei besonders spezialisierten Dienstleistungen im Gesundheitsbereich stellt.[185] Gerade der zuletzt angesprochene Punkt ist für die innovative bayerische Wirtschaft wichtig. Denn den Ideen im Bereich E-Health sind keine Grenzen gesetzt. So erforscht beispielsweise der US-Konzern Google derzeit eine spezielle digitalisierte Kontaktlinse für Diabetiker, die den Blutzuckerspiegel misst und zur ständigen Verfügbarkeit und Selbstkontrolle an das Smartphone des Nutzers überträgt.[186] Einem Unternehmen, welches ein

---

[179] Vgl. Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 17. Aufl. 2017, § 4a BDSG, Rn. 1; a.A. Riesenhuber, RdA 2011, 257, 258 (tatbestandsausschließendes Einverständnis).
[180] Scheja/Haag, in: Münchener Anwaltshandbuch IT-Recht, 3. Aufl. 2013, Teil 5. Datenschutzrecht, Rn. 78.
[181] Vgl. OLG Hamm, Urt. v. 20.09.2012 - I-4 U 85/12.
[182] Hierzu ausführlich Kühling/Seidel, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 96 ff.
[183] Vgl. Schmidl, IT-Recht von A-Z, 2. Aufl. 2014, S. 158.
[184] Kühling, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, § 4a BDSG Rn. 62. Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[185] BSG, Beschl. v. 10.12.2008 - B 6 KA 37/07 mit Anm. Berger, jurisPR-ITR 10/2009, Anm. 5.
[186] https://www.welt.de/gesundheit/article123943259/Google-Labor-arbeitet-an-Kontaktlinse-fuer-Diabetiker.html (zuletzt abgerufen am 02.08.2017);

derartiges Medizinprodukt vermarktet, sollte klar sein, dass der Betroffene regelmäßig allein schon deswegen in den Umgang mit seinen Patientendaten einwilligt, damit ihm nicht der Genuss der E-Health-Innovation verwehrt bleibt.

Praxistipp

Anzustreben ist stets eine Entkoppelung der Akteure im Gesundheitswesen, sobald Einwilligungen der Betroffenen einzuholen sind. Ist eine Entkopplung nicht möglich, sollte der Leistungsträger etwa auf die Einbeziehung einer externen Abrechnungsstelle verzichten. Eine datenschutzkonforme Lösung kann dann in der Direkt-Abrechnung mit dem Patienten liegen.[187]

Noch nicht höchstrichterlich geklärt ist das Problem, ob noch Freiwilligkeit angenommen werden kann, wenn vom Betroffenen aufgrund äußerer Umstände, etwa kurz vor einer Operation, nicht erwartet werden kann, dass er gezielt seine Daten preisgibt.[188] Das OLG Celle hat 2009 immerhin entschieden, dass die Entschließungsfreiheit des Betroffenen unzumutbar eingeschränkt ist, wenn er nach zweistündiger Behandlung Vertragsunterlagen zur Unterschrift vorgelegt bekommt.[189] Freiwilligkeit bedinge vielmehr einen gewissen zeitlichen und räumlichen Abstand zwischen Vertragsabschluss und Behandlung, der im vorgenannten Beispiel nicht gegeben sei.

Praxistipp

Auch im E-Health-Bereich sollte – soweit möglich – auf eine zeitliche und räumliche Entzerrung geachtet werden, damit die Freiwilligkeit der Einwilligung nicht gefährdet ist. Vorzugsweise sollte die Einwilligung daher noch im Anbahnungsverhältnis des E-Health-Vertrages eingeholt werden.[190]

---

http://www.computerworld.com/article/3066870/wearables/why-a-smart-contact-lens-is-the-ultimate-wearable.html (zuletzt abgerufen am 02.08.2017).

[187] Kühling, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, § 4a BDSG Rn. 62.

[188] Kühling, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, § 4a BDSG Rn. 63.

[189] OLG Celle, Urt. v. 11.09.2008 - 11 U 88/08.

[190] Vgl. Kühling, in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, § 4a BDSG Rn. 63.

4.2.2 Einwilligung bei Big Data-Anwendungen[191]

Bei Big Data-Anwendungen ist der Anwendungsbereich der datenschutzrechtlichen Einwilligung sehr eingeschränkt. Für jede E-Health-Anwendung müsste zunächst separat geklärt werden, ob die Einwilligung überhaupt den Eingriff rechtfertigen kann und ob nicht ein anderer Erlaubnistatbestand Vorrang genießt. Bei der Einwilligung müsste jeder Betroffene allerdings vollumfänglich darüber informiert werden, was mit seinen Daten geschieht. Gerade bei Big Data-Analysen stellen sich hierbei allein aufgrund der Menge der Betroffenen einige Herausforderungen. Bei den hier in Frage stehenden Gesundheitsdaten kommt – wie bereits aufgezeigt –hinzu, dass es sich um eine besondere Kategorie personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG handelt, sodass sich die Einwilligung nach § 4a Abs. 3 BDSG ausdrücklich auf die Erhebung, Verarbeitung oder Nutzung der Gesundheitsdaten beziehen muss.[192] Dennoch erscheint bei Wahrung der Transparenzvorgaben gerade auch eine mittels informierter Einwilligung datenschutzrechtlich gerechtfertigte Erweiterung von Small Data- auf Big Data-Anwendungen jedenfalls nicht von Vornherein ausgeschlossen.[193]

---

[191] Vgl. hierzu Timm, MedR 2016, 686 ff.; Brus/Schwab, Medizinische Einsatzmöglichkeiten von Big Data oder Big Data im Gesundheitswesen - am Datenschutz erkrankt? in: Taeger (Hrsg.), Tagungsband DSRI-Herbstakademie 2014, S. 171; Becker/Schwab, ZD 2015, 151 ff.
[192] Becker/Schwab, ZD 2015, 151, 153.
[193] Vgl. hierzu die vbw Studie „Big Data im Freistaat Bayern – Chancen und Herausforderungen“, 2016, S. 110.

4.2.3 (Kaum) Änderungen unter der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung, die ab dem 25.05.2018 unmittelbar[194] in allen EU-Mitgliedstaaten gilt, behält die Einwilligung als zentralen Erlaubnistatbestand bei. Anders als das BDSG verbietet die neue EU-Verordnung jedoch die Verarbeitung „besonderer Kategorien personenbezogener Daten". Hierzu zählen wiederum die Gesundheitsdaten, jedoch lässt die Datenschutz-Grundverordnung in ihrem Art. 9 Abs. 2 Ausnahmen zu. Eine dieser Ausnahmen ist die aus dem BDSG bekannte ausdrückliche Einwilligung. Allerdings werden an deren Wirksamkeit hohe Voraussetzungen geknüpft. Im Einzelnen:[195]

- Die Einwilligung setzt eine unmissverständliche, ausdrückliche Handlung voraus.

Praxistipp

Der Verordnungsgeber hat sich durchaus bemüht, die Datenschutz-Grundverordnung technikfreundlich zu gestalten und ist bei den Formerfordernissen weitaus weniger restriktiv als das BDSG. Eine unmissverständliche, ausdrückliche Handlung bedeutet daher nicht notwendigerweise Schriftform (vgl. § 4a Abs. 1 Satz 1 BDSG), sondern kann grundsätzlich auch in einem Mausklick liegen.[196]

- Der Betroffene muss noch vor der Datenverarbeitung über sein jederzeitiges Widerrufsrecht, die Identität des Verarbeiters und die Verarbeitungszwecke informiert werden.
- Einwilligungserklärungen, die Teil von Allgemeinen Geschäftsbedingungen sind, müssen deutlich hervorgehoben werden. Der Verwender muss sich einer klaren und unmissverständlichen Sprache bedienen.
- Auch unter der Datenschutz-Grundverordnung gilt das Kopplungsverbot weiter, sodass vertragliche Einwilligungserklärungen unwirksam sind, soweit sie sich auf Gesundheitsdaten erstrecken, welche zur Vertragserfüllung nicht benötigt werden.
- Schließlich wird die Einwilligung in die Verarbeitung von Gesundheitsdaten dadurch erschwert, dass sie im Falle eines klaren Ungleichgewichts zwischen Betroffenem und Verantwortlichem nicht wirksam zustande kommt. An der hierdurch geforderten Gleichordnung zwischen den Beteiligten fehlt es etwa

---

[194] „Unmittelbar" meint ohne weiteren Umsetzungsakt.
[195] Hierzu ausführlich Härting, Datenschutz-Grundverordnung, 2016, S. 88 f.
[196] Beispiel nach Härting, Datenschutz-Grundverordnung, 2016, S. 88.

dann, wenn datenverarbeitende staatliche oder öffentliche Stellen aus einem Über-Unterordnungsverhältnis heraus mit dem Betroffenen agieren.[197]

4.3 Rechtskonformitäts-Check für Gesundheits-Apps

Die Tatsache, dass die Digitalisierung im Gesundheitswesen angekommen ist, zeigt sich deutlich an einer Fülle neuer Mobile Health- (kurz: mHealth) Produkte für Verbraucher. Sogenannte Erinnerungs-Apps unterstützen den Patienten darin, regelmäßig seine Medikamente einzunehmen.[198] Ernährungs-Apps bewahren ihre Nutzer vor ungewollter Kalorienaufnahme, etwa[199] indem sie ihm im Supermarkt mithilfe eines Barcodescans genaue Kalorien-Angaben zu den einzelnen Nahrungsmitteln in den Regalen liefern. Fitness-Apps ersetzen teure Fitnesskurse.[200] Den Ideen der Entwickler sind nahezu keine Grenzen gesetzt, vor allem, wenn zusätzliche Hardware (z.B. Blutzuckermessgeräte) eingesetzt wird. Werden die Datensätze (z.B. die Blutzuckerwerte) an den behandelnden Arzt zur weiteren Verwendung übermittelt, spricht man in Fachkreisen von Remote Diagnostic.[201] Inzwischen haben auch die Krankenkassen das Potential des mHealth-Bereichs für sich entdeckt und bieten ihrerseits entsprechende Apps zum Download an.[202] Der Anbieter einer solchen App hat allein schon aus Haftungs- und Imagegründen ein großes Interesse daran, seine App möglichst rechtskonform auszugestalten.

Praxistipp

Eine Aussage darüber, ob eine konkrete App tatsächlich rechtskonform ausgestaltet ist, lässt sich stets nur nach einer Einzelfall-Überprüfung – ggf. durch einen beauftragten Rechtsanwalt – tätigen. Allerdings können dem App-Anbieter nachfolgend bestimmte Kriterien im Sinne eines Rechtskonformitätschecks aufgezeigt werden, welche in jedem Fall zu beachten sind.

Hinzuweisen ist noch darauf, dass die nachstehenden Gesichtspunkte zum einen nicht den Kauf entsprechender Apps als solchen betreffen bzw. die mit dem Vertrieb zu-

---

[197] Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 9 Rn. 24 m.w.N.
[198] Beispiel: die App „Pillenalarm“ der Bayer AG, vgl. hierzu https://www.bayer.de/de/apps-von-bayer.aspx (zuletzt abgerufen am 02.08.2017).
[199] Beispiel: die App des US-Konzerns Weight Watchers, vgl. hierzu https://weightwatchers.com/de/weight-watchers-online-so-geht-abnehmen-heute (zuletzt abgerufen am 02.08.2017).
[200] Beispiele unter: http://www.spiegel.de/gesundheit/ernaehrung/sechs-fitness-apps-im-test-training-mit-dem-smartphone-a-1037094.html (zuletzt abgerufen am 02.08.2017).
[201] Bidgoli, The Handbook of Technology Management, Vol. 2, 2010, S. 116.
[202] Vgl. etwa https://bayern.aok.de/leistungen-services/services/aok-apps/ (zuletzt abgerufen am 02.08.2017); https://www.tk.de/tk/tk/tk-apps/209048 (zuletzt abgerufen am 02.08.2017).

sammenhängenden Fragen wie etwa einer ggf. erforderlichen Berücksichtigung des Heilmittelwerberechts; vielmehr soll die rechtskonforme Ausgestaltung der App beleuchtet werden. Zum anderen müssen Unternehmer weitere (verbraucher-) rechtliche Bestimmungen berücksichtigen, sofern sie in ihren Apps Möglichkeiten des Vertragsschlusses vorhalten (sogenannte In-App-Käufe), etwa mit Blick auf ihre Allgemeinen Geschäftsbedingungen, Preisangaben und weitere Informationspflichten gegenüber Verbrauchern beispielweise über deren Widerrufsrechte.[203]

4.3.1 CE-Kennzeichnung (Medizinproduktrecht)

Eine Gesundheits-App ist als Medizinprodukt im Sinne des Medizinproduktegesetzes (MPG) einzuordnen, wenn sie durch ein Scoring-Modul zu einer Entscheidung über eine Diagnose bzw. Therapie verhilft, Labordaten mit Referenzdaten abgleicht oder für den Nutzer ein Medikationsmodul enthält.[204] Handelt es sich bei einer Gesundheits-App um ein Medizinprodukt im vorbeschriebenen Sinne, ist die CE-Kennzeichnung nach § 6 MPG für ihr Inverkehrbringen und ihre Inbetriebnahme erforderlich. Die CE-Kennzeichnung ist ihrerseits allerdings an strenge Voraussetzungen geknüpft (§ 6 Abs. 2 MPG); in einem Konformitätsbewertungsverfahren muss der Hersteller nachweisen, dass sein Produkt den gesetzlichen Anforderungen genügt. Neben dem Hersteller sind auch sämtliche Zwischenhändler Adressaten der CE-Kennzeichnungspflicht im Hinblick auf das Inverkehrbringen der entsprechend kennzeichnungspflichtigen Apps.[205]

Praxistipp

Bayerische App-Hersteller, die unsicher sind, ob ihr Produkt eine CE-Kennzeichnung benötigt, um in den Verkehr gebracht werden zu können, sollten ihr örtlich zuständiges Gewerbeaufsichtsamt konsultieren.[206] Dies kann straf- bzw. ordnungswidrigkeitenrechtliche Sanktionen vermeiden sowie Schadens- und Unterlassungsansprüchen von Mitbewerbern vorbeugen.[207]

---

[203] Vgl. hierzu ausführlich den vbw Leitfaden „Online-Vertrieb und Online-Marketing“, dort 1.
[204] So ausdrücklich Rübsamen, MedR 2015, 485, 487.
[205] Lücker, in: Spickhoff, Medizinrecht, 2. Aufl. 2014, § 6 MPG Rn. 3.
[206] Vgl. Wagner, in: Rehmann/Wagner, MPG, 2. Aufl. 2010, § 26 Rn. 10.
[207] Vgl. Rübsamen, MedR 2015, 485, 487.

4.3.2 Name der App (Markenrecht)

Die Bezeichnung einer (Gesundheits-)App ist grundsätzlich dem Werktitelschutz fähig, vgl. § 5 Abs. 3 MarkenG.[208] Werktitelschutz kann zwar erst dann erlangt werden, wenn die erforderliche originäre Kennzeichnungskraft vorliegt, d.h. das Zeichen „von Haus aus“ unterscheidungskräftig ist,[209] Gesundheits-App-Anbieter sollten sich der markenrechtlichen Problematik dennoch bewusst sein. Eine frühzeitige und gründliche Markenrecherche im Markenregister des Deutschen Patent- und Markenamts[210] – gegebenenfalls durch einen beauftragten Rechtsanwalt – kann vorbeugen, dass die Bezeichnung der neuen Gesundheits-App Markenrechte Dritter verletzt. Letzteres kann wiederum Unterlassungs- und/oder Schadensersatzansprüche des jeweiligen Markenrechtsinhabers nach sich ziehen.

4.3.3 Datenschutzrecht

Aufgrund der vielen gesundheitsbezogenen Daten, die bei einer Gesundheits-App anfallen, den vielfältigen Ebenen, die bei der Verwendung dieser Daten berührt werden und der Vielzahl an beteiligten Akteuren, ist bei diesen Anwendungen auf das Thema Datenschutz ein besonderes Augenmerk zu legen.[211]

4.3.3.1 Allgemeine datenschutzrechtliche Vorgaben

Freilich müssen sich auch Anbieter von Gesundheits-Apps an die datenschutzrechtlichen Grundprinzipien wie etwa das Gebot der Datensparsamkeit bzw. Datenminimierung halten (siehe im Einzelnen unter III.4.a). Dabei ist bereits bei der Entwicklung von Gesundheits-Apps auf Privacy by design, also datenschutzfreundliche Voreinstellungen, zu achten.[212]

Datenschutzrechtliche Erlaubnistatbestände für die Verwendung von Gesundheitsdaten als besonders geschützte Daten gem. § 3 Abs. 9 BDSG (z.B. Gewicht, Blutzuckerwerte, Röntgenbilder) finden sich in den Absätzen 6 bis 9 des § 28 BDSG. Da diese allerdings nur sehr spezielle Anwendungsfälle, wie z.B. die Bewusstlosigkeit des Betroffenen (§ 28 Abs. 6 Nr. 1 BDSG), regeln, werden sie im Bereich der Gesundheits-Apps nur selten zum Tragen kommen.[213] Sofern eine App zur medizinischen Versorgung z.B. durch Ärzte verwendet wird, kommt § 28 Abs. 7 BDSG in Betracht; in diesem

---

[208] LG Hamburg, Beschl. v. 08.10.2013 - 327 O 104/13.
[209] LG Hamburg, Beschl. v. 08.10.2013 - 327 O 104/13.
[210] https://register.dpma.de/ (zuletzt abgerufen am 02.08.2017).
[211] Rübsamen, MedR 2016, 485, 487.
[212] Rübsamen, MedR 2016, 485, 488.
[213] Ortner/Daubenbüchel, NJW 2016, 2918, 2920.

Fall können allerdings zusätzlich landesrechtliche Datenschutzbestimmungen zu beachten sein.[214]

Weiterhin können die Vorgaben des Sozialdatenschutzes einschlägig sein, sofern Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person von einer in § 35 Abs. 1 SGB I genannten Stelle im Hinblick auf ihre Aufgaben erhoben, verarbeitet oder genutzt wird, § 67 Abs. 1 SGB X. Insbesondere die Leistungsträger, also vornehmlich Krankenkassen, sind daher zur Wahrung des Sozialgeheimnisses verpflichtet.[215]

Apps stellen zudem ein „Telemedium" im Sinne des TMG dar, sodass in Bezug auf die sogenannten Bestands- und Nutzungsdaten wie Name, E-Mail-Adresse und IP-Adresse des App-Nutzers auch in jedem Fall die bereichsspezifischen Vorschriften des Telemediengesetzes (TMG) zu beachten sind, konkret die §§ 12 ff. TMG.[216]

Sofern kein gesetzlicher Tatbestand den Umgang mit den Daten rechtfertigt, ist auf die Einwilligung durch den Betroffenen, mithin den Nutzer der Gesundheits-App, zurückzugreifen, sofern die Daten nicht anonymisiert oder pseudonymisiert (§ 3 Abs. 6, 6a BDSG) werden.[217] Die Einwilligung muss nicht zwangsläufig das Schriftformerfordernis wahren. Eine elektronische Einwilligung reicht im Telemedien-Datenschutzrecht nach § 13 Abs. 2 TMG aus, wenn folgende Voraussetzungen kumulativ vorliegen:

- Der App-Nutzer erteilt die Einwilligung bewusst und vor allem eindeutig.
- Die Einwilligung wird protokolliert.
- Der Nutzer kann den Inhalt seiner Einwilligungserklärung jederzeit abrufen.
- Der Nutzer kann die einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen.

---

[214] Rübsamen, MedR 2016, 485, 488.
[215] Lücking, in: Sodan, Handbuch des Krankenversicherungsrechts, 2. Aufl. 2014, § 41 Rn. 13.
[216] So auch Alich, Dr. App? – Rechtliche Aspekte von Gesundheits- und Medizin-Apps, in: Taeger (Hrsg.), IT und Internet – mit Recht gestalten, Tagungsband DSRI-Herbstakademie 2012, S. 570 f.
[217] Rübsamen, MedR 2015, 485, 488.

4.3.3.2 Mit Geltung der EU-Datenschutzgrundverordnung ab Mai 2018 erfährt der datenschutzrechtliche Rechtsrahmen mit Blick auf die Verarbeitung von Gesundheitsdaten keine gravierenden Veränderungen zum bisherigen Recht.[218] Relevant mit Blick auf Gesundheits-Apps ist jedoch, dass ab diesem Zeitpunkt die bereichsspezifischen Vorgaben des Telemedienrechts, mithin die §§ 11 ff. TMG, weitgehend nicht mehr zur Anwendung kommen werden.[219] Nachdem jedoch elektronische Einwilligungserklärungen bereits durch die EU-DSGVO selbst ermöglicht werden,[220] ergibt sich aber auch insoweit keine Änderung für die Anbieter von Gesundheits-Apps.Datenschutzerklärung

§ 13 Abs. 1 TMG verpflichtet jeden App-Anbieter dahingehend, die Nutzer der App zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten in allgemein verständlicher Form zu unterrichten.[221] Bei einem automatisierten Verfahren, welches eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer spätestens zu Beginn dieses Verfahrens zu unterrichten. Es kommt also auf die Funktionsweise der Gesundheits-App an. Verwendet die App personenbezogene Daten[222], muss eine Datenschutzerklärung den Nutzer hierüber umfassend und transparent aufklären. Diese muss bereits im App-Store aufrufbar sein und den Nutzer erstmals über die Verwendungsvorgänge in Kenntnis setzen, da bereits bei der Installation der App eine Datenverarbeitung stattfinden kann, in die der Nutzer zuvor einwilligen muss.[223]

Praxistipp

Auch eine dynamische IP-Adresse kann für den Telemedien-Diensteanbieter (App-Anbieter) ein personenbezogenes Datum sein. Dies setzt voraus, dass er über rechtliche Mittel verfügt, welche es ihm erlauben, die Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.[224]

---

[218] Siehe bereits unter 4.1.2.
[219] Vgl. Keppeler, MMR 2015, 779, 781; Marosi, One (smart) size fits all? – Das (Datenschutz-)TMG heute – und morgen?, in: Taeger (Hrsg.), Smart World - Smart Law?, Tagungsband DSRI-Herbstakademie 2016, S. 435, 450; Schantz, NJW 2016, 1841; v.Schenck/Mueller-Stöfen, GWR 2017, 171, 177; Ziegenhorn, NVwZ 2017, 216, 218.
[220] Siehe bereits unter 4.1.3.
[221] Vgl. hierzu https://upload-magazin.de/blog/11371-recht-und-datenschutz-fuer-mobile-apps/ (zuletzt abgerufen am 02.08.2017).
[222] Zum Begriff der personenbezogenen Daten siehe unter 3.4.1.
[223] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil F., Rn. 20.
[224] EuGH, Urt. v. 19.10.2016 - C-582/14 (Breyer/Deutschland).

Inhaltlich muss die Datenschutzerklärung im Einzelnen Informationen zu folgenden Punkten enthalten:[225]

- umfängliche Angaben zur verantwortlichen Stelle
- Informationen über die Datenverarbeitung durch die App
- Funktionsweise der App auf dem Endgerät
- Angaben zum Zweck der Datenverarbeitung durch die App
- konkrete Benennung Dritter, sofern an diese Daten übermittelt werden
- Eingriffsmöglichkeiten des Nutzers im Hinblick auf die Datenverarbeitung
- Auswirkungen der Einwilligungsverweigerung auf die Funktionalität der App
- Angaben zur Datenübermittlung an Drittstaaten außerhalb des Europäischen Wirtschaftsraumes (EWR)

Auf Grund der zahlreichen notwendigen Informationen und der beschränkten Darstellungsmöglichkeiten auf Smartphones und Tablets empfiehlt sich eine Untergliederung in einzelne Kapitel.[226] Unter Umständen kann es ausreichend sein, im Rahmen der Datenschutzerklärung auf dem Endgerät lediglich die wesentlichen Inhalte aufzuführen und bezüglich weitergehender Hinweise einen gut sichtbaren Link auf eine externe Quelle zu setzen.

Hinsichtlich der Form der Datenschutzerklärung ist anzuführen, dass diese für den Nutzer auch nach Beginn des Nutzungsvorgangs jederzeit leicht auffindbar und abrufbar sein muss. Unter Umständen kann es ausreichend sein, die Datenschutzerklärung auf der Angebotsseite des jeweiligen App-Stores zu platzieren, sofern diese über die App erreichbar ist.[227] Auch die Verlinkung auf eine externe Website kann dem Gebot der Auffindbarkeit und Abrufbarkeit genügen.[228] Zwar muss die Erklärung als solche leicht und ohne Hindernisse auffindbar sein, sie bedarf jedoch nicht zwingend der Betitelung als „Datenschutzerklärung“.[229] Zu beachten ist weiterhin, dass die Datenschutzerklärung, sofern sie mit weiteren Erklärungen, wie z.B. den Nutzungsbedingungen[230], verbunden wird, ebenfalls der AGB-rechtlichen Inhaltskontrolle nach den §§ 305 ff. BGB unterfallen kann.[231]

Wie bereits dargestellt, werden aufgrund des Anwendungsvorrangs des EU-Rechts ab dem 25.05.2018 die §§ 11 ff. TMG und damit auch § 13 Abs. 1 TMG aller Voraussicht

---

[225] Nach: Baumgartner, in: Baumgartner/Ewald, Apps und Recht, 2. Aufl. 2016, Kap. 5 Rn. 232.
[226] Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 18 ff., https://www.lda.bayern.de/media/oh_apps.pdf (zuletzt abgerufen am 02.08.2017). Der nachfolgende Text bezieht sich ebenso auf diese Quelle.
[227] Lachenmann, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2015, IX. Datenschutzerklärungen, 7. Datenschutzerklärungen für mobile Apps.
[228] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil F., Rn. 21.
[229] Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 18, https://www.lda.bayern.de/media/oh_apps.pdf (zuletzt abgerufen am 02.08.2017).
[230] Siehe hierzu unter 4.3.6.
[231] Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht. 2. Aufl. 2016, § 28 Rn. 58.

nach unangewendet bleiben müssen. Jedoch sieht die EU-Datenschutzgrundverordnung in den Art. 12-14 vergleichbare Transparenzanforderungen vor, welche sich jedoch nicht speziell auf Telemedien beziehen. Besonders erwähnenswert mit Blick auf die europäischen Neuregelungen erscheint dabei der Fokus auf eine klare und einfache Sprache in Art. 12 Abs. 1 Satz 1 EU-DSGVO, welcher auch bei der Anpassung bzw. Erstellung von Datenschutzerklärungen für Gesundheits-Apps zu beachten ist. Die besonderen Anforderungen im Kontext der Telemedien sollen überdies auf europäischer Ebene demnächst mittels der geplanten „Verordnung über Privatsphäre und elektronische Kommunikation“ (sog. ePrivacy-Verordnung) geregelt werden.[232]

4.3.3.3 Übermittlung von Daten in die USA

Nicht selten übermitteln Unternehmen im Bereich Gesundheits-Apps Daten in die USA, etwa weil sich die Server des gewählten Cloud-Dienstleisters dort befinden. Die (datenschutz-)rechtskonforme Ausgestaltung dieses Datentransfers sollten Unternehmen daher stets im Blick haben. Negativ-Schlagzeilen machten zuletzt etwa die Unternehmen Adobe, Punica und Unilever. Letztgenannte hatten weiter personenbezogene Daten auf Grundlage des sogenannten Safe Harbor-Abkommens in die USA übermittelt, obschon 2015 der EuGH in der Rechtssache Schrems[233] den Angemessenheitsbeschluss der Kommission hinsichtlich Safe Harbor für rechtswidrig erklärt hatte. Mittels eines Angemessenheitsbeschlusses stellt die EU Kommission fest, dass ein Drittland ein mit der Europäischen Union vergleichbares Datenschutzrecht gewährleistet. Für die USA wurde dies im Jahr 2000 in begrenzten Umfang für Unternehmen festgestellt, die dem Safe Harbor Programm beitraten.[234]

Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit (HmbBfDI) verhängte gegen Adobe, Punica und Unilever Bußgelder bis zu einer Höhe von 11.000 Euro.[235] Theoretisch wären derzeit Bußgelder bis hin zu 300.000 Euro möglich. Der Image-Schaden dürfte jedoch weitaus größer sein. Mit Geltung der EU-DSGVO erhöht sich der mögliche Bußgeldrahmen um ein Vielfaches auf bis zu 4% des weltweit erzielten Jahresumsatzes des Unternehmens bzw. 20 Millionen Euro – je nachdem, welcher Betrag höher ist. Die Anbieter von Gesundheits-Apps sollten daher kritisch überprüfen, auf welcher Rechtsgrundlage sie Daten in die USA übermitteln.

---

[232] Vgl. den Verordnungsvorschlag der Europäischen Kommission v. 10.01.2017, COM(2017) 10 final.
[233] EuGH, Urt. v. 06.10.2015 - C-362/14 mit Anm. Heckmann/Starnecker, JM 2016, 58 ff.; Kamps/Bonanni, ArbRB 2015, 334; Seiler, jurisPR-BKR 11/2015, Anm. 2.
[234] Determann/Weigl, EuZW 2016, 811.
[235] https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-datenuebermittlungen-in-die-usa.html?tx_ttnews Prozent5BbackPid Prozent5D=1&cHash=f00d844fb3434a4d32451675b0c454a5 (zuletzt abgerufen am 02.08.2017).

Anfang 2016 hatte sich die EU-Kommission mit den USA auf einen neuen Rechtsrahmen für den transatlantischen Datentransfer geeinigt, das „EU-US Privacy-Shield".[236] Am 12.07.2016 verabschiedete die Kommission offiziell den Angemessenheitsbeschluss.[237] Im Vergleich zu Safe Harbor müssen die teilnehmenden US-Unternehmen strengere Anforderungen bei der Weiterübermittlung von Daten erfüllen.[238] Aufsicht hierüber führt die Federal Trade Commission[239] (FTC). Der Privacy Shield enthält darüber hinaus eine schriftliche Zusicherung der US-Nachrichtendienste, dass EU-Bürger nicht massenhaft überwacht werden. Letztere erhalten im Rahmen des Privacy Shields die Möglichkeit, sich mit Anfragen oder Beschwerden an eine spezielle Ombudsstelle zu wenden. Seit 01.08.2016 können interessierte US-Unternehmen die Selbstzertifizierung in der Privacy Shield List beantragen. Eine Liste zertifizierter Unternehmen ist unter https://www.privacyshield.gov/list[240] zugänglich.

Ob der Angemessenheitsbeschluss zum Privacy Shield einer Überprüfung durch den EuGH standhält, ist offen. Die Kritik am Privacy Shield reißt zumindest nicht ab.[241] Es ist nicht auszuschließen, dass der EuGH ähnlich wie in der Rechtssache Schrems[242] entscheidet und auch diesen Angemessenheitsbeschluss für ungültig erklärt.

Praxistipp

Nachdem die Rechtslage – wie dargestellt – bislang noch nicht abschließend geklärt ist, ist den betroffenen Unternehmen mit Blick auf ihren transatlantischen Datenverkehr zur Verwendung der EU-Standardvertragsklauseln zu raten.[243] Generell ist es – wie bereits ausgeführt – von besonderer Wichtigkeit für Unternehmer, gerade im Hinblick auf diese Thematik die Datenflüsse im Unternehmen und deren Rechtsgrundlagen einer regelmäßigen Überprüfung zu unterziehen. Nicht nur an dieser Stelle empfiehlt sich wiederum die Einholung qualifizierten Rechtsrates. Überdies kommt das Bayerische Landesamt für Datenschutzaufsicht seinem Beratungsauftrag u.a. mit einer um-

---

[236] http://europa.eu/rapid/press-release_IP-16-433_en.htm (zuletzt abgerufen am 02.08.2017).
[237] Durchführungsbeschluss (EU) 2016/1250 der Kommission v. 12.07.2016 gemäß der RL 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 v. 01.08.2016, S. 1.
[238] Ausführlich zu den Änderungen durch das Privacy Shield siehe v.Lewinski, EuR 2016, 412 ff.
[239] https://www.ftc.gov/ (zuletzt abgerufen am 02.08.2017).
[240] Zuletzt abgerufen am 09.08.2017.
[241] http://www.heise.de/newsticker/meldung/Privacy-Shield-Buergerrechtler-schiessen-scharf-gegen-geplanten-Datenschutzschild-3093494.html (zuletzt abgerufen am 02.08.2017).
[242] EuGH, Urt. v. 06.10.2015 - C-362/14 mit Anm. Heckmann/Starnecker, JM 2016, 58 ff.; Kamps/Bonanni, ArbRB 2015, 334; Seiler, jurisPR-BKR 11/2015 Anm. 2.
[243] Abrufbar im Anhang unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF (zuletzt abgerufen am 02.08.2017).

fangreichen Informationssammlung zum internationalen Datentransfer auf seiner Website nach.[244]

4.3.4 Impressum

Bei einer App handelt es sich um ein „Telemedium“ im Sinne des TMG. Weitere Voraussetzung der Pflicht zur Anbieterkennzeichnung (sog. Impressumspflicht) ist die sog. Geschäftsmäßigkeit der angebotenen App. Viele Gesundheits-Apps werden „kostenlos“ zum Download angeboten; der Nutzer der App bezahlt in diesem Fall ausschließlich mit seinen Daten. Auch solche Angebote dürften jedoch der Impressumspflicht unterfallen.[245] Dies folgt bereits aus dem Wortlaut von § 5 TMG, wonach Geschäftsmäßigkeit vorliegt, wenn „in der Regel“ ein Entgelt verlangt wird. Das heißt, die Entgeltlichkeit ist gerade nicht zwingende Voraussetzung. Vom Anwendungsbereich ausgenommen ist vielmehr allein das rein private Angebot.[246] Auch das Vorhandensein einer Gewinnerzielungsabsicht ist in diesem Kontext nicht vonnöten.[247] Damit unterfallen Gesundheits-Apps in aller Regel der telemedienrechtlichen Pflicht zur Anbieterkennzeichnung.

Das Impressum muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein sowie dabei alle in § 5 TMG vorgesehenen Informationen zum Diensteanbieter verfügbar halten. Hierzu gehören der Name und die Anschrift des Diensteanbieters, eine E-Mail-Adresse zur schnellen elektronischen Kontaktaufnahme und unmittelbaren Kommunikation mit ihm sowie ein diesen Vorgaben entsprechender zweiter Kommunikationskanal[248], etwa in Form einer Festnetz-Telefonnummer, die Post-Anschrift seiner zuständigen Aufsichtsbehörde, bei Personenvereinigungen, welche in einem der im Gesetz genannten Register verzeichnet sind, zudem die jeweilige Registerbehörde sowie die Registernummer, gegebenenfalls berufsspezifische Angaben (nur bei den reglementierten Berufen), schließlich noch die Umsatzsteuer-ID. Besonderheiten bestehen noch für Unternehmen in der Abwicklung oder Liquidation.

Neben dem TMG enthält § 55 Abs. 1 des Rundfunkstaatsvertrages (RStV) eine besondere Kennzeichnungsregelung für Anbieter von Telemedien, die zwar in Abgrenzung zu § 5 TMG nicht regelmäßig gegen Entgelt erbracht werden, aber dennoch „nicht ausschließlich“ persönlichen oder familiären Zwecken dienen (sogenanntes „kleines Impressum“[249]). § 55 Abs. 1 RStV kommt damit gegenüber § 5 TMG ein insoweit eigen-

[244] Abrufbar unter https://www.lda.bayern.de/de/international.html (zuletzt abgerufen am 09.08.2017).
[245] Vgl. Bräutigam, MMR 2012, 635, 638, der die Preisgabe personenbezogener Daten als gleichwertiges Austauschgut sieht.
[246] BT-Drs. 16/3078, S. 14.
[247] Ott, in: BeckOK Informations- und Medienrecht, 16. Edition, Stand: 01.05.2017, § 5 TMG Rn. 9.
[248] Weiterführend hierzu Leeb/Starnecker, AnwZert ITR 17/2016, Anm. 2.
[249] Jandt, in: Bräutigam/Rücker, E-Commerce, 2017, 10. Teil C., Rn. 12.

ständiger Anwendungsbereich zu.[250] Da aber jedenfalls davon auszugehen ist, dass – wie aufgezeigt – Gesundheits-Apps in aller Regel dem Anwendungsbereich von § 5 TMG unterfallen und dieser ohnehin ein „Mehr“ an Kennzeichnungspflichten gegenüber § 55 Abs. 1 RStV enthält, dürfte § 55 Abs. 1 RStV für Anbieter solcher Apps in aller Regel keine praktische Rolle spielen. Darüber hinaus sieht § 55 Abs. 2 RStV besondere Angaben vor, wenn das Angebot journalistisch-redaktionell gestaltet ist. App-Anbieter müssen dann über die Angaben in § 5 TMG hinaus einen Verantwortlichen für die journalistisch-redaktionellen Inhalte mit Angabe seines Namens und seiner Anschrift im Impressum benennen. Bei Gesundheits-Apps kann den Anbieter eine solche Pflicht beispielsweise dann treffen, wenn über die App neben einem reinen Datendienst auch noch gesundheitliche oder medizinische Informationen und Nachrichten bereitgestellt werden.

Gerade beim Angebot entsprechender Apps kann es auf Grund der technisch eingeschränkten Darstellungsmöglichkeiten auf Smart Devices wie Smartphones und Tablets zu Schwierigkeiten bei der pflichtgemäßen Anbieterkennzeichnung kommen.[251] Für die „unmittelbare Erreichbarkeit“ wird es dementsprechend bei Apps regelmäßig genügen, wenn auf das Impressum im „Hauptmenü“ der App verwiesen wird[252] und das Hauptmenü durch einfaches Scrollen zu erreichen ist.[253]

Praxistipp

Die vorstehenden Angaben können nur als Richtwert dienen. Im Zweifel empfiehlt es sich, einen Rechtsanwalt einzuschalten, der ein passgenaues Impressum erstellt. Unternehmen ist insbesondere von der Verwendung kostenloser Textbausteine aus dem Internet – zumindest ohne jegliche Anpassung – abzuraten. Selbiges gilt gerade auch für die Datenschutzerklärung (siehe hierzu unter 4.3.3.2).

4.3.5 Vorgaben des App-Store-Betreibers

Bei der Entwicklung von Apps sind weiterhin die Vorgaben der App-Store-Betreiber zu beachten, da diese die Plattform anbieten, von welcher aus die Apps vertrieben werden.[254] Die Rechtsbeziehungen zwischen dem App-Anbieter und dem App-Store-Betreiber werden in der Regel durch die Standardvertragsbedingungen des jeweiligen

---

[250] Vgl. Held, in: Hahn/Vesting, Rundfunkrecht, 3. Aufl. 2012, § 55 RStV Rn. 26.
[251] Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 28 Rn. 22.
[252] Ewald, in: Baumgartner/Ewald, Apps und Recht, 2. Aufl. 2016, Kap. 4 Rn. 168.
[253] Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 28 Rn. 22.
[254] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil F., Rn 19.

Anbieters definiert.[255] Abhängig vom Betreiber können sich diese signifikant unterscheiden,[256] enthalten aber zumeist Bestimmungen zur Laufzeit des Vertrages, zum Zulassungsvorbehalt des Store-Betreibers, zu Compliance sowie umfangreiche Haftungsfreistellungen des Store-Betreibers.[257] Da diese überwiegend US-amerikanische Unternehmen darstellen, allen voran Apple und Google, finden die strengen deutschen AGB-Regelungen in den §§ 305 ff. BGB im Verhältnis zwischen den Betreibern und den Anbietern der App nur sehr begrenzt Anwendung.[258] Dies hat im Ergebnis zur Folge, dass die Anbieter vor die Wahl gestellt werden, die gegebenen Bedingungen zu akzeptieren oder auf den jeweiligen Marktzugang zu verzichten.[259] Von besonderer Bedeutung für den App-Anbieter ist, dass die App-Store-Betreiber, bevor sie die App in ihr Angebot aufnehmen, diese regelmäßig umfangreich prüfen und gegebenenfalls auch zurückweisen können.[260]

Hat sich der App-Anbieter für die jeweilige Plattform entschieden, muss er die Vorgaben des Store-Betreibers weiter im Blick haben. So finden sich auch zum Datenschutz Vorgaben in den einzelnen Vertragsbedingungen, beispielsweise verpflichtet die Richtlinie des Google-Play-Store[261] die Entwickler zur Kenntlichmachung der Datenverarbeitung und zum sicheren Umgang mit personenbezogenen Daten.[262] Dabei kommt es auf den jeweiligen Store-Betreiber an, ob die genannten Vertragsbedingungen über die gesetzlichen Vorgaben hinausgehende inhaltliche Compliance-Anforderungen an den jeweiligen App-Anbieter stellen oder nicht.

4.3.6 Eigene Nutzungsbedingungen

Den App-Entwicklern ist es in der Regel gestattet, ergänzend zu den Nutzungsbedingungen des jeweiligen App-Stores, eigene allgemeine Vertragsbedingungen zur Regelung des Verhältnisses Entwickler-Nutzer zu erstellen.[263] Es empfiehlt sich innerhalb dieser Bedingungen, zum Nutzungsumfang der App, zur Gewährleistung und zu haftungsrechtlichen Fragen Stellung zu nehmen.[264] Dabei sind allerdings die Bestimmun-

---

[255] Solmecke/Taeger/Feldmann, Mobile Apps – Rechtsfragen und rechtliche Rahmenbedingungen, 2013, Rn. 167.
[256] Ewald, in: Baumgartner/Ewald, Apps und Recht, 2. Aufl. 2016, Kap. 3 Rn. 93.
[257] Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 28 Rn. 13.
[258] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil C., Rn. 3.
[259] Solmecke/Taeger/Feldmann, Mobile Apps – Rechtsfragen und rechtliche Rahmenbedingungen, 2013, Rn. 169.
[260] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil C., Rn. 5.
[261] Abrufbar unter: https://play.google.com/intl/de_ALL/about/developer-content-policy/ (zuletzt abgerufen am 02.08.2017).
[262] Ziffer 4.3 der Google Play Vereinbarung für den Entwicklervertrieb, https://play.google.com/intl/ALL_de/about/developer-distribution-agreement.html (zuletzt abgerufen am 02.08.2017).
[263] Zdanowiecki, in: Bräutigam/Rücker, E-Commerce, 2017, 11. Teil C., Rn. 28.
[264] https://upload-magazin.de/blog/11371-recht-und-datenschutz-fuer-mobile-apps/ (zuletzt abgerufen am 02.08.2017).

gen über die allgemeinen Geschäftsbedingungen der §§ 305 ff. BGB zu beachten.[265] Probleme können sich dabei insbesondere bei der wirksamen Einbeziehung der AGB in den Vertrag ergeben.[266] Gem. § 305 Abs. 2 Nr. 2 BGB muss der *anderen Vertragspartei die Möglichkeit verschafft werden, in zumutbarer Weise […] vom Inhalt der allgemeinen Geschäftsbedingungen Kenntnis zu nehmen*. Die Zumutbarkeit der Kenntnisnahme von umfangreichen AGB auf kleinen (Smartphone-)Displays darf zumindest bezweifelt werden, eine anderweitige Kenntnisnahme zum Beispiel über den Ausdruck der entsprechenden AGB ist praktisch kaum möglich.[267] Daher sollten sich Unternehmer insoweit – ggf. unter Zuhilfenahme anwaltlicher Beratung – um kurze Formulierungen bemühen.

4.4 Big Data-Analysen von Gesundheitsdaten

Unter einer Big Data-Analyse wird eine Datenanalyse verstanden, die es gestattet, riesige Datenmengen aus einer Vielzahl von Quellen mit einer hohen Verarbeitungsgeschwindigkeit zu kombinieren und hieraus neue Erkenntnisse zu ziehen.[268] Die Wirtschaft sieht in Big Data-Analysen daher schon die Raffinerien für das „new oil".[269] Auch im Gesundheitssektor ist Big Data angekommen und hilft, hochwertigere Ergebnisse zu erzielen als mit herkömmlichen Analysemethoden. Mittels Big Data kann etwa ein konkreter Krankheitsfall mit Unmengen anderer gespeicherter Krankheitsverläufe von anderen Patienten abgeglichen werden, sodass am Ende eine gezielte Diagnose und Medikation steht.[270] Ein bekanntes Beispiel für Big Data-Analysen sind die Google Grippe-Trends.[271] Der Suchanbieter Google kann anhand eingegebener Suchanfragen die Ausbreitung einer Grippe-Welle präzise vorhersagen.

Zentraler Aufhänger für die datenschutzrechtliche Diskussion zu Big Data-Analysen ist wiederum das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983: Jedem Einzelnen stehe nach dem Recht auf informationelle Selbstbestimmung zu, „grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen".[272] Big Data befindet sich nun in einem (scheinbaren) Widerspruch zum bereits beschriebenen Zweckbindungsgrundsatz und dem Prinzip der Datensparsamkeit, welche dem Grundrecht auf informationelle Selbstbestimmung immanent sind.[273] Denn

---

[265] Solmecke/Taeger/Feldmann, Mobile Apps – Rechtsfragen und rechtliche Rahmenbedingungen, 2013, S. 149.
[266] Dazu ausführlich Janal, NJW 2016, 3201 ff.
[267] Janal, NJW 2016, 3201, 3205.
[268] Vgl. Becker/Schwab, ZD 2015, 151.
[269] http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#5439207b77a9 (zuletzt abgerufen am 02.08.2017).
[270] Vgl. Becker/Schwab, ZD 2015, 151.
[271] http://www.ndr.de/nachrichten/netzwelt/Wie-aussagekraeftig-ist-der-Google-Grippe-Trend,grippetrends100.html (zuletzt abgerufen am 02.08.2017).
[272] BVerfG, Urt. v. 15.12.1983 - 1 BvR 209/83 u.a.
[273] Vertiefend Heckmann, in: Byrd/Hruschka/Joerden, Jahrbuch für Recht und Ethik, 23. Bd. 2015, S. 17 ff.

eine funktionierende Big Data-Analyse setzt ja gerade voraus, dass eine Vielzahl von Daten für alle denkbaren Zwecke angesammelt und vorgehalten wird.

Aus übergeordneten Interessen des Allgemeinwohls lässt der Gesetzgeber allerdings Ausnahmen von den vorgenannten Grundsätzen zu, nämlich die gesetzlichen Erlaubnistatbestände, wozu insbesondere die §§ 28 ff. BDSG bzw. Art. 6 ff. EU-DSGVO zählen. Da es sich bei Gesundheitsdaten um eine besondere Kategorie personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG bzw. Art. 4 Nr. 15 EU-DSGVO handelt, könnte eine Big Data-Analyse insofern nur auf die sehr restriktiven Sonderregelungen der §§ 28 Abs. 6-9, 29 Abs. 5 BDSG bzw. Art. 9 EU-DSGVO sowie §§ 22 ff. BDSG-neu gestützt werden. Die Restriktivität dieser Regelungen wird deutlich, wenn man sich den – im Wesentlichen durch Art. 9 Abs. 2 lit. c EU-DSGVO fortgeführten – Wortlaut von § 28 Abs. 6 Nr. 1 BDSG vor Augen führt: *„zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich“*. Eine ähnliche Formulierung enthält Art. 9 Abs. 2 lit. c EU-DSGVO. Hiernach könnte z.B. auf Patientendaten zurückgegriffen werden, um etwaige gesundheitliche Risiken bei einer Bluttransfusion bei einem Angehörigen auszuschließen.[274] Mögliche Einsatzbereiche im Kontext von Big Data-Anwendungen können etwa die personalisierte Medizin oder auch die Medikamentenforschung betreffen.

Liegt allerdings ein gesetzlicher Erlaubnistatbestand nicht vor, können Gesundheitsdaten nur mit einer ausdrücklichen Einwilligung der Betroffenen verwendet werden. Wie bereits dargestellt, bereitet bei Big Data-Analysen insbesondere das Merkmal hinreichender Informiertheit rechtskonformer Einwilligungen häufig Schwierigkeiten. Diese Voraussetzung ist etwa dann nicht gewahrt, wenn in einem ersten Schritt eine pauschale Erfassung aller verfügbaren Daten erfolgt und diese so lange vorgehalten werden, bis diese in einem zweiten Schritt mittels „passender“ Big Data-Anwendung einer Auswertung zugeführt werden können.[275] Dies bedeutet jedoch nicht, dass eine Wertschöpfung durch derartige neue Analysemethoden in jedem Einzelfall von Vornherein ausgeschlossen ist, sofern die Anbieter entsprechender Analyse-Tools einen Weg finden, den Transparenzanforderungen hinreichend beizukommen.[276]

Praxistipp

Datenschutzrechtlich unproblematisch ist – neben der Verarbeitung von ausschließlich sachbezogenen Daten – die Arbeit von Big Data-Anwendungen mit anonymisierten

[274] Becker/Schwab, ZD 2015, 151, 152.
[275] Lüdemann, ZD 2015, 247, 251.
[276] Siehe hierzu bereits unter 4.1.2 sowie die vbw Studie „Big Data im Freistaat Bayern – Chancen und Herausforderungen“, 2016, S. 110.

Daten (im Sinne von § 3 Abs. 6 BDSG).[277] Anonymisierung ist eine inhaltliche Umgestaltung personenbezogener Daten derart, dass der Personenbezug tatsächlich oder faktisch nicht mehr hergestellt werden kann.[278] Zu beachten ist jedoch, dass die Anonymisierung von Gesundheitsdaten im Regelfall nur mit Einwilligung des Betroffenen zulässig ist.[279]

Eine große technische Herausforderung für die Anbieter von Big Data-Anwendungen dürfte überdies darin bestehen, sicherzustellen, dass die einmal erfolgte Anonymisierung der Daten bestehen bleibt. Denn durch die ständig hinzukommenden neuen Datensätze lässt sich womöglich im Rahmen einer Rekombination der Personenbezug wiederherstellen.[280]

---

[277] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 3.
[278] Schulz, in: BeckOK BDSG, 20. Edition, Stand: 01.11.2014, § 3a BDSG Rn. 72.
[279] Siehe hierzu bereits unter 3.4.1.
[280] Spindler, MedR 2016, 691 f.

5 Ausblick

Diskussion zu ethischen Problemstellungen nötig

Mensch oder Maschine? Welche Rolle spielt der moderne Patient im Fokus eines digitalisierten Gesundheitswesens? Wie kann ein IT-*b*etriebenes und IT-*ge*triebenes Gesundheitswesen ein menschliches Antlitz bewahren? Avanciert der Mensch im E-Health der nächsten 10, 20 Jahre zum reinen Datenlieferanten einer hocheffizienten Gesundheitsvorsorge? Big Data – Big Brother? Es geht um mehr als technische Innovation zwischen Usability und Compliance – es geht um ethische Grundfragen einer freiheitlichen Gesellschaft.

Wie viel Kommerzialisierung und Determinierung darf mit der Entwicklung eines elektronischen Gesundheitswesens einhergehen? Damit können zwei Ebenen unterschieden werden, die man pointiert mit Digitalisierung des Medizinischen einerseits und Medizinierung des Digitalen andererseits bezeichnen könnte: Auf der einen Ebene geht es um die Digitalisierung der medizinischen Informationen und Verfahren, was im 21. Jahrhundert eine Selbstverständlichkeit sein sollte. Die Ausstattung hochmoderner Arztpraxen, Operationssäle und Intensivstationen zeigt zumindest in Deutschland und anderen modernen Ländern die Vorteile des technischen Fortschritts für Gesundheitsvorsorge und Lebensrettung. Was hier begonnen wurde, soll im Internetzeitalter fortgesetzt werden: durch Telemedizin, Teleoperationen und eine bessere Zugänglichkeit und Validität der maßgeblichen Gesundheitsdaten. Auf der anderen Ebene geht es um die permanente digitale Erfassung des Lebensalltags und zunehmende massenhafte Analyse von Gesundheitsdaten, was in Zeiten von Social Media und Self-Improvement auf das Lebensgefühl vieler Menschen trifft. Dennoch ist nicht alles, was unter dem Label „E-Health“ gesundheitsfördernd angeboten wird, es wert, die Hoheit über unser gesundheitsrelevantes Verhalten an IT-Dienstleister abzutreten. Gesundheitsdaten sollten keine Handelsware sein.

Ob und inwieweit mit dem letztgenannten Aspekt zusammenhängende Geschäftsmodelle legitim sein können: Das bedarf einer offen und transparent geführten gesellschaftlichen Debatte, die von den politischen Akteuren initiiert und gelenkt werden muss. Eine solche ergebnisoffene Diskussion sollte sich – bezogen auf den Bereich des digitalen Gesundheitswesens – auch auf eine flächendeckende Gesundheitsvorsorge durch Analyse von Gesundheitsdaten beziehen. Sowohl die mit E-Health-Anwendungen verbundenen erheblichen Chancen als auch die hierdurch entstehenden Risiken müssen in diesem Zusammenhang ausreichend zur Sprache kommen. Hierzu leistet etwa der Deutsche Ethikrat einen wesentlichen Beitrag. Die Aktualität und Brisanz der darin diskutierten Fragestellungen zeigt alleine ein Blick auf die Themen seiner letzten Jahrestagungen: 2015 fand diese zum Thema „Die Vermessung des Menschen – Big Data und Gesundheit“ statt, „Zugriff auf das menschliches Erbgut. Neue Möglichkeiten und ihre ethische Beurteilung“ sowie „Autonome Systeme. Wie intelligente Maschinen uns verändern“ waren die Themen der Jahre 2016 und 2017.

Abbildungsverzeichnis

Alle Abbildungen wurden durch den Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht der Universität Passau, Herr Prof. Dr. Dirk Heckmann, erstellt.

Ansprechpartner

Franz Niedermaier
Abteilung Sozial- und Gesellschaftspolitik

Telefon 089-551 78-224
Telefax 089-551 78-213
franz.niedermaier@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich grundsätzlich sowohl auf die weibliche als auch auf die männliche Form. Zur besseren Lesbarkeit wurde meist auf die zusätzliche Bezeichnung in weiblicher Form verzichtet.

Herausgeber:

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Weiterer Beteiligter:

Prof. Dr. Dirk Heckmann

Lehrstuhl für Öffentliches Recht,
Sicherheitsrecht und Internet-
recht
Universität Passau
0851/509-2290
heckmann@mein-jura.de