Spitzenverband

Beitrag des GKV-Spitzenverbandes vom 13.09.2016

zur Öffentlichen Konsultation zur Sicherheit von Apps und anderer nicht eingebetteter Software

GKV-Spitzenverband
Reinhardtstraße 28, 10117 Berlin
Telefon 030 206288-0
Fax 030 206288-88
politik@gkv-spitzenverband.de
www.gkv-spitzenverband.de
Transparenzregister-Nummer
839750612639-40

I. Einleitung

Die Europäische Kommission hat am 09.06.2016 eine Konsultation zur Sicherheit von Apps und anderer nicht eingebetteter Software eingeleitet. Sie betrifft unter anderem Apps für Gesundheit und Wohlergehen. Ziel ist, nächste Schritte und politische Maßnahmen auf EU-Ebene zu definieren und horizontale oder auch sektorspezifische Rechtsvorschriften anzupassen.

Der GKV-Spitzenverband begrüßt, dass die Europäische Kommission die Sicherheit von Apps thematisiert. Denn Gesundheits-Apps, Medizin-Apps und Medizinprodukte-Apps bergen neben Potentialen auch unterschiedliche Niveaus an Sicherheitsrisiken. Sie können gesundheitliche Schäden verursachen oder deren Beseitigung verzögern, beispielsweise wenn sie fehlerhaft oder unzuverlässig arbeiten, fehlerhaft angewendet werden oder wirkungslos sind. Denkbar sind darüber hinaus wirtschaftliche Schäden und Sachschäden sowie Risiken bei der Datensicherheit.

Aus Sicht des GKV-Spitzenverbandes decken existierende horizontale und sektorspezifische EU-Rechtsvorschriften die Sicherheit von Gesundheits-Apps und anderer nicht-eingebetteter Software nicht ausreichend ab. Aufgrund des potenziell grenzüberschreitenden Charakters der Verarbeitung und Nutzung von Gesundheitsdaten sind zusätzliche (einheitliche) Regelungen für die Datensicherheit notwendig. Auch muss durch europaweit gültige Regelungen eindeutig geklärt sein, dass Apps unter die Medizinprodukterichtlinie 93/42 EWG bzw. die zukünftige EU-Medizinprodukte-Verordnung fallen, wenn ihre Zweckbestimmung der Initiierung oder Steuerung medizinischer Therapien dient, durch sie eine medizinische Diagnose vergeben wird oder ihre Anwendung gemäß der Zweckbestimmung einer Screening- oder Präventionsmaßnahme gleichkommt.

Der GKV-Spitzenverband vertritt alle 117 gesetzlichen Kranken- und Pflegekassen in Deutschland und damit die Interessen der über 70 Millionen Versicherten und Beitragszahlenden gegenüber Politik und Leistungserbringern. Er berät die Parlamente und Ministerien im Rahmen aktueller Gesetzgebungsverfahren und nimmt als gesetzliche Aufgabe die Interessen der Kranken- und Pflegekassen bei über- und zwischenstaatlichen Organisationen und Einrichtungen wahr. Er ist über die Deutsche Sozialversicherung (DSV) in der European Social Insurance Platform (ESIP) organisiert.

II. Beitrag zur Konsultation

1. Welche Arten von Apps oder sonstiger nicht eingebetteter Software stellen Sicherheitsrisiken dar? Bitte führen Sie Beispiele an.

Gesundheits-Apps, Medizin-Apps und Medizinprodukte-Apps, teilweise mit medizinischen Geräten oder mit Sensoren (z. B. in Armbändern oder Uhren) vernetzt, wie auch persönliche Hinweis- bzw. Begleitsysteme, per SMS übermittelte Gesundheitsinformationen und Erinnerungen an die Medikamenteneinnahme sowie drahtlos bereitgestellte Telemedizindienste können ein Sicherheitsrisiko darstellen. Darüber hinaus bestehen App-Angebote zur Abwicklung von Geschäftsprozessen der Krankenversicherung. Durch die Verknüpfung mit den IT-Systemen der Krankenversicherer bestehen Anforderungen an die IT- und Informationssicherheit dieser Systeme.

Unterschiedliche Kategorien dieser Apps bergen neben Potentialen auch unterschiedliche Niveaus an Sicherheitsrisiken. Zu unterscheiden sind Gesundheit-Apps, medizinische Apps und Medizinprodukte-Apps sowie Apps zur Abbildung von Geschäftsprozessen in der Krankenversicherung.

- Apps zur Abwicklung von Geschäftsprozessen nutzen elektronische Daten der Versicherten und ersetzen somit zunehmend papiergebundene Prozesse im Rahmen der Digitalisierung. Durch den Charakter der oftmals als Sozialdaten einzustufenden Inhalte unterliegen diese Verfahren höchsten Schutzanforderungen.
- Gesundheits-Apps sind mobile Anwendungen für Bürgerinnen und Bürger sowie Patientinnen und Patienten mit dem primären Ziel der Gesundheitsförderung (Lucht et al., 2015).
- Medizin-Apps umfassen mobile Anwendungen für Leistungserbringer zur Unterstützung des Berufsalltags, sowie mobile Anwendungen für Patientinnen und Patienten zum besseren Selbstmanagement meist chronischer Erkrankungen (Lucht et al., 2015).
- Medizinprodukte-Apps dienen dem Erkennen, Verhüten, Überwachen, der Behandlung oder Linderung von Krankheiten, dem Erkennen, Überwachen, der Behandlung, Linderung oder Kompensation von Verletzungen oder Behinderungen, der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder der Empfängnisverhütung (§ 3, Nr. 1 Gesetz über Medizinprodukte, MPG).

2. Was für eine Art von Risiko können Apps oder andere nicht-eingebettete Software darstellen?

X Wirtschaftliche Schäden

X Personenschäden

X Sach- und Vermögensschäden

X Immaterielle Schäden (Schmerz und Leid)

X Anderes

Führen Sie dies bitte aus:

In unterschiedlicher Weise sind die oben genannten Arten von Apps bzw. nicht eingebetteter Software potenziell geeignet, gesundheitliche Schäden zu verursachen oder deren Beseitigung zu verzögern, beispielsweise wenn sie fehlerhaft oder unzuverlässig arbeiten, fehlerhaft angewendet werden oder wirkungslos sind.

In verschiedenen Quellen ist dokumentiert, dass bei den hier adressierten Arten von Apps oder Software ein fehlerhaftes Funktionieren vorkommt. Beispiele sind etwa:
Unkorrekte Eingaben durch Nutzerinnen und Nutzer werden nicht zurückgewiesen, z. B. bei Diabetes-Apps, die Insulindosen berechnen (Huckvale et al., 2015), oder Parameter der Körperfunktion werden nicht korrekt gemessen, sodass keine validen Ergebnisse für den Energieumsatz des Körpers (Murakami et al., 2016) oder für den Blutdruck (Plante et al., 2016) produziert werden. Unter Umständen kann eine fehlerhaft kalkulierte Insulindosis oder ein als normal angezeigter, in Wirklichkeit zu hoher Blutdruckwert zu einem Personenschaden führen. Apps zur Beurteilung von Hautveränderungen können fehlerhafte diagnostische Einschätzungen produzieren (Wolf et al., 2013). Dass solche Fehleinschätzungen Kosten durch weitere Inanspruchnahmen zur Abklärung der Verdachtsdiagnosen sowie immaterielle Schäden (Schmerz und Leid) produzieren, ist naheliegend. Insofern eine Fehleinschätzung diagnostisch oder therapeutisch eingesetzter Apps zu einer Nicht-Inanspruchnahme notwendiger medizinischer Versorgung führt, können auch Personenschäden oder Fehldiagnosen- oder Therapien entstehen.

Potenziell besteht auch das Risiko wirtschaftlicher Schäden, wenn Nutzerinnen und Nutzern Kosten durch die Nutzung von unsicheren oder schadhaften Gesundheits-Apps entstehen oder diese durch die gesetzliche Krankenversicherung (GKV) erstattet werden. Die Erbringung ambulanter Leistungen durch Mobile-Health-Dienste ist grundsätzlich im Rahmen der Regelversorgung zu Lasten der GKV möglich. Hierbei ist deren Wirtschaftlichkeit, auch im Vergleich zu bereits zu Lasten der Krankenkassen erbrachten Methoden, zu berücksichtigen (siehe auch Frage 10).

Ein wesentlicher Aspekt ist das Risiko der Datensicherheit. Gesundheitsdaten gehören zu den sensibelsten personenbezogenen Daten und bedürfen des besonderen Schutzes. Grundvoraussetzung für die sichere Verarbeitung von Gesundheitsdaten durch Mobile-Health-Dienste sind eine Ende-zu-Ende-Verschlüsselung, klare Zugriffsrechte, eine sichere Authentifizierung der Zugriffsberechtigten sowie die Verwendung sicherer Endgeräte. Das Risiko des unberechtigten Zugriffs auf Gesundheitsdaten oder gar deren Weitergabe sowie Manipulationsmöglichkeit sind so weit als möglich zu minimieren.

Sach- und Vermögensschäden können aus der technischen Kompromittierung von IT-Systemen der Dienstanbieter entstehen. Je nach Art eines Schadangriffes können Kosten für die Wiederherstellung von Systemen, Kosten für einen Ausgleich von Schadenersatzansprüchen oder aber auch Kosten für die Information der betroffenen Kunden entstehen. Bei schwerwiegenden Angriffen ist

nicht auszuschließen, dass IT-Systeme vollständig abgeschrieben werden müssen, z. B. aktuelle Vorfälle bei Krypto-Trojanern.

Bitte geben Sie Ihre Meinung zu den folgenden Optionen:

	Kein Risiko	Niedriges Risiko	Hohes Risiko	Sehr hohes Risiko
Wirtschaftliche Schäden	○	X	○	○
Personenschäden	○	○	X	○
Sach- und Vermögensschäden	○	○	X	○
Immaterielle Schäden (Schmerz und Leid)	○	○	X	○
Anderes	○	X	○	○

Führen Sie dies bitte aus:

Je nach App oder Software können die Risiken, die mit der Anwendung einhergehen unterschiedlich hoch sein. Eine Insulin-App, die falsche Dosen des Medikaments kalkuliert, kann ein sehr hohes Risiko darstellen. Ein Schrittzähler, der ungenau zählt, stellt ein eher geringes oder kein Risiko für den Nutzer dar. Zu wirtschaftlichen und Sach- und Vermögensschäden und dem Risiko der Datensicherheit siehe oben.

3. In welchen Sektoren sind Apps und nicht-eingebettete Software am meisten von Sicherheitsrisiken betroffen?

- ○ Landwirtschaft
- ○ Elektronische Kommunikation/Telekommunikation
- X Gesundheit
- ○ Hausautomation

Bitte führen Sie dies näher aus:

Apps und nicht-eingebettete Software im Gesundheitssektor können Sicherheitsrisiken bergen. Zu Sicherheitsrisiken von Apps in anderen Sektoren äußert sich der GKV-Spitzenverband nicht.

4. Haben Sie in Ihrer beruflichen Erfahrung unsichere Apps oder andere nicht-eingebettete Software entdeckt oder haben sich Konsumenten an Sie gewandt, da diese Probleme mit unsicheren Apps oder anderer nicht-eingebetteter Software hatten?

X Ja

○ Nein

Bitte führen Sie dies näher aus:

In den Quellen (Huckvale et al., 2015; Murakami et al., 2016; Plante et al., 2016) sind konkrete Apps benannt.

4.1. Falls ja: Was haben Sie unternommen, um diese Probleme zu lösen?

Bislang liegt es an der Initiative engagierter wissenschaftlicher Autorinnen und Autoren, Reviews zu verfassen, wie etwa Huckvale et al., 2015. Auf der Grundlage dieses Artikels hat die Medicines and Healthcare products Regulatory Agency (MRHA) des Vereinigten Königreichs die einzelnen Hersteller der fehlerhaften Apps angeschrieben und zu Stellungnahmen aufgefordert. Aus Deutschland liegen keine Informationen über Interventionen infolge des Bekanntwerdens von fehlerhaft arbeitenden Apps vor.

Im Bereich der gesetzlichen Krankenversicherung in der Bundesrepublik wird im Rahmen der Digitalisierung zunehmend auf Mechanismen des E-Government gesetzt. Dazu wird über Bundesgesetze der Handlungsspielraum für Anbieter von Apps klar geregelt. Die Aufsichtsbehörden definieren auf dieser Grundlage klare Anforderungen an das Angebot von Apps. Dabei werden insbesondere Mechanismen im Bereich IT- und Informationssicherheit auf Grundlage von Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik geprüft.

5. Sind existierende EU oder nationale Sicherheitsvorschriften und Marktüberwachungsmechanismen ausreichend, um unsichere Apps und andere nicht-eingebettete Software zu überwachen und, wenn nötig, vom Markt zu nehmen?

○ Ja

X Nein

Führen Sie dies bitte aus:

Auf nationaler Ebene sind dem GKV-Spitzenverband bezüglich der Produktsicherheit Sicherheitsvorschriften für solche Apps bekannt, die durch das Medizinproduktegesetz (MPG) reguliert sind.

Hinsichtlich IT-und Informationssicherheit für Apps in der gesetzlichen Krankenversicherung bestehen ausreichende Grundlagen auf nationaler Ebene. Dieses sind: (aus ADV-Prüfleitfaden Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten, Stand 22.04.2016)

- BSI-Standard 100-1 bis 100-4
- BSI IT-Grundschutzkataloge
- Technische Richtlinie TR03138 „Ersetzendes Scannen“ (TR-RESISCAN)
- Technische Richtlinie TR03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ (TR-ESOR)
- „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ (BfDI vom 01.03.2013)
- „Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (BMI Referat O2 – Stand: 27.06.2013)
- Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – Leitlinien und gemeinsame Maßstäbe für IuK-Prüfungen, Stand: November 2011
- Organisationskonzept elektronische Verwaltungsarbeit (Herausgeber: Bundesministerium des Innern)
- Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden (Version 1.0, Stand 2014)

Zu EU-Vorschriften siehe Antwort zu Frage 7.

6. Wurden Sie bereits für Schäden, die Konsumenten aufgrund von unsicheren Apps/nicht-eingebetteter Software entstanden, in Verantwortung gezogen?

- ○ Ja, als Hersteller des Geräts, auf welchem die Software läuft oder welches sie kontrolliert
- ○ Ja, als Entwickler/Hersteller von Apps oder Software
- ○ Ja, als Händler oder Zwischenhändler (z.B. App Store)
- ○ Ja, sonstiges
- X Nein

6.1. Falls ja: Was haben Sie gemacht?

Keine Antwort

7. Glauben Sie, dass existierende horizontale und sektorspezifische EU Rechtsvorschriften (z.B. Produktsicherheitsrichtlinie, Marktüberwachungsverordnung, Medizinprodukterichtlinie, Funkanlagenrichtlinie) zusammengenommen die Sicherheit von allen Arten von Apps und anderer nicht-eingebetteter Software ausreichend abdecken?

- ○ Ja
- X Nein

Bitte führen Sie dies aus:

Datensicherheit:
Grundvoraussetzung für die sichere Verarbeitung von Gesundheitsdaten durch Mobile-Health-Dienste sind eine Ende-zu-Ende-Verschlüsselung, klare Zugriffsrechte, eine sichere Authentifizierung der Zugriffsberechtigten sowie die Verwendung sicherer Endgeräte.

Aufgrund des grenzüberschreitenden Charakters der Verarbeitung und Nutzung von Gesundheitsdaten sind zusätzliche (einheitliche) Regelungen notwendig. Es muss transparent sein, zu welchen Zwecken Daten erhoben und genutzt werden, wann und ob sie gelöscht werden, wenn die App deinstalliert wird und wo die Daten gespeichert werden.

Zulassung und Produktsicherheit:
Eine klare Unterscheidung zwischen Medizinprodukten und Gesundheits- bzw. Medizin-Anwendungen ist wichtig. Mobile Anwendungen zur Erfassung von Messwerten, wie z. B. Herzfrequenz beim Belastungssport, sind zwar im weitesten Sinne dem Bereich „Lebens- und Ernährungsberatung" zuzuordnen (Trainingsplaner, Nahrungsmittel-Kalorienrechner usw.), sie messen jedoch gesundheitlich und medizinisch bedeutsame Parameter mit einem wissenschaftlichen Anspruch an die Validität der Messwerte.

Eine mHealth-Anwendung wird zu einem Medizinprodukt, wenn ihre Zweckbestimmung der Initiierung oder Steuerung medizinischer Therapien dient, durch sie eine medizinische Diagnose vergeben wird oder ihre Anwendung gemäß der Zweckbestimmung einer Screening- oder Präventionsmaßnahme gleichkommt. Unter dem Begriff „medizinische Therapie" können neben der Verordnung und Anpassung von Arzneimitteltherapien auch konkrete personalisierte Diätpläne zu verstehen sein. Screening oder Prävention in dem genannten Sinne wäre beispielweise eine Smartphone-App, die aufgrund von Fotos das Entartungsrisiko von Hautläsionen abschätzt (vgl. Wolf et al. Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection. JAMA Dermatol 2013, 149: 422-426).

In diesem Zusammenhang besteht Handlungsbedarf. Es muss durch europaweit gültige Regelungen eindeutig geklärt sein, dass Apps mit einer solchen Zweckbestimmung unter die Medizinprodukterichtlinie 93/42 EWG bzw. die zukünftige EU-Medizinprodukte-Verordnung fallen. Der GKV-Spitzenverband fordert deshalb eine unabhängige Prüfung der Leistungsmerkmale der Softwareprodukte durch eine Benannte Stelle, zur Sicherstellung der Wirksamkeit und Funktionstauglichkeit der Produkte sowie einer transparenten Information über ihre Leistungen und Risiken. Eine reine „Selbsterklärung" der Hersteller, wie bei Medizinprodukten der Risikoklasse I, reicht für mobile Gesundheitsanwendungen nicht aus, wenn sie einer Zweckbestimmung im vorher genannten Sinne für Therapie, Diagnose, Screening oder Prävention entsprechen.

Apps müssen nach dem Risiko klassifiziert werden, das mit ihrer Nutzung zusammenhängt und nach Maßgabe dieses Risikos auf Qualität geprüft werden. Außerdem muss ihr Nutzen für die Patientinnen und Patienten und ihre Kosteneffektivität in der Therapie nachgewiesen werden. Die Regel 10a zur Klassifikation aktiver Geräte im konsolidierten Kompromisstext der neuen EU-Medizinprodukte-Verordnung (Fassung vom 27.06.2016) sieht vor, dass Software der Klasse IIa zuzuordnen ist, wenn sie Informationen bereitstellen soll, die für diagnostische oder therapeutische Entscheidungen genutzt werden. Kann eine solche Entscheidung direkt oder indirekt eine ernsthafte Verschlechterung des Gesundheitszustandes oder eines chirurgischen Eingriffs bewirken, so ist die Software der Klasse IIb zuzuordnen. Kann eine solche Entscheidung gar zum Tod

oder einer irreversiblen Verschlechterung des Gesundheitszustandes führen, wird die Software der Klasse III zugeordnet.

Software zum Überwachen physiologischer Prozesse ist laut Entwurf der Verordnung der Klasse IIa zuzuordnen, es sei denn, es handelt sich um die Überwachung von vitalen physiologischen Parametern, deren Änderung zu einer unmittelbaren Gefahr für die Patienten führen könnte. In diesem Fall handelt es sich um ein Produkt der Klasse IIb. Jegliche andere Software fällt in die Klasse I.

Diese Präzisierung bei der Einordnung von Gesundheits-Apps in die jeweiligen Produktklassen erhöht ein Stück weit die Sicherheit im Umgang mit Apps dieser Definition.

Zum Zeitpunkt des Inverkehrbringens muss gewährleistet sein, dass sich der Nutzer öffentlich über die geprüfte Leistungsfähigkeit der mobilen Anwendung informieren kann.

Für die gesetzliche Krankenversicherung ist es von sehr hoher Bedeutung, dass die bestehenden Haftungsregelungen nicht aufgeweicht werden. Im Schadensfall müssen die geltenden Bestimmungen der Produkthaftung auf Seiten der Hersteller vor allem von Medizinprodukten zur Anwendung kommen, um bestehende Schadensersatzansprüche von Versicherten und Patienten zu erfüllen.

10. Gibt es in dem EU-Land, in dem Sie tätig sind, spezielle Regeln für Sicherheitsanforderungen in Bezug auf Apps oder andere nicht eingebettete Software?

X Ja

○ Nein

Soweit in Deutschland Apps von Krankenkassen oder anderen Sozialversicherungsträgern angeboten werden, reicht mit Blick auf die Nutzung von Sozialdaten die nationale Gesetzgebung in § 35 SGB I, den §§ 67 ff. SGB X und z. B. § 284 SGB V aus. Dort wird hinreichend streng geregelt, zu welchen Zwecken Sozialdaten genutzt werden dürfen und wie Einwilligungen zu gestalten sind. Sollte eine App, die Sozialdaten abfragt, auftragsweise für eine Krankenkasse erstellt und betrieben werden, ist die Auftragserteilung nur unter den strengen Voraussetzungen des § 80 SGB X möglich.

Für Medizinprodukte-Apps sind Angaben über die Zweckbestimmung gesetzlich vorgeschrieben. Die Zweckbestimmung ist die Verwendung, für die das Medizinprodukt in der Kennzeichnung, der

Gebrauchsanweisung oder den Werbematerialien nach den Angaben des Herstellers bestimmt ist (§ 3 Abs. 1 Nr. 10 Medizinproduktegesetz, MPG). Diese erfolgt durch Selbsterklärung der Hersteller nach § 5 MPG.

Die Erbringung ambulanter Leistungen durch Mobile-Health-Dienste (in diesem Zusammenhang nach § 87 Abs. 2a Satz 8 SGB V als ambulante telemedizinische Leistungen bezeichnet) ist grundsätzlich auch im Rahmen der Regelversorgung zu Lasten der GKV möglich. Wann es sich um telemedizinische Leistungen handelt und welche Voraussetzungen für eine Kostentragung durch die GKV erfüllt sein müssen, kann der Rahmenvereinbarung (Anlage) entnommen werden. Für den Fall, dass es sich bei der telemedizinischen ambulanten Leistung um eine neue Untersuchungs- oder Behandlungsmethode handelt, muss außerdem zunächst der Gemeinsame Bundesausschuss Empfehlungen abgegeben haben über

1) die Anerkennung des diagnostischen und therapeutischen Nutzens der neuen Methode sowie deren medizinische Notwendigkeit und Wirtschaftlichkeit – auch im Vergleich zu bereits zu Lasten der Krankenkassen erbrachten Methoden – nach dem jeweiligen Stand der wissenschaftlichen Erkenntnisse in der jeweiligen Therapierichtung,
2) die notwendige Qualifikation der Ärzte, die apparativen Anforderungen sowie Anforderungen an Maßnahmen der Qualitätssicherung, um eine sachgerechte Anwendung der neuen Methode zu sichern, und
3) die erforderlichen Aufzeichnungen über die ärztliche Behandlung (§ 135 Abs. 1 SGB V).

Die Speicherung von Sozialdaten in Clouds ist nicht zulässig. Beim Betreiben von mobilen Gesundheitsdiensten durch Dritte für Krankenkassen ist sicherzustellen, dass die Anbieter ausreichend kontrolliert werden (wie es u. a. § 80 SGB X vorsieht). Verarbeitung und Speicherung von Gesundheitsdaten in ungeschützten „Cloud"-Systemen sind äußerst problematisch.

13. Weitere Kommentare

Das von einer Erkrankung ausgehende Risiko sollte weder durch den sozialen Status des Erkrankten, noch durch seine regionale Einbettung und Mobilität sowie den damit einhergehenden Zugang zu medizinischer Versorgung beeinflusst werden.

Vor diesem Hintergrund ist es wichtig, trotz gebotener Vorsicht die Chancen von Mobile-Health-Diensten herauszustellen (Dorsey et al., 2016). Diese können bei einer integrativen Einbettung in das bestehende Versorgungssystem, einer strikten Beachtung geltender Datenschutzbedingungen, wissenschaftlich evidentem Inhalt und unabhängiger Qualitätssicherung eine Möglichkeit sein, bestehende Defizite zu adressieren.

14. Evidenz, Referenzen (Dateien zum Hochladen)

- Rahmenvereinbarung zwischen der Kassenärztlichen Bundesvereinigung und dem GKV-Spitzenverband als Trägerorganisationen des Bewertungsausschusses gemäß § 87 Abs. 1 Satz 1 SGB V zur Überprüfung des Einheitlichen Bewertungsmaßstabes gemäß § 87 Abs. 2a Satz 8 SGB V zum Umfang der Erbringung ambulanter Leistungen durch Telemedizin.
- Dorsey, E.R., Topol, E.J., 2016. State of Telehealth. N ENGL J MED 375; 2. DOI: 10.1056/NEJMral1601705.
- Huckvale, K., Adomaviciute, S., Prieto, J.T., Leow, M.K.-S., Car, J., 2015. Smartphone apps for calculating insulin dose: a systematic assessment. BMC Med. 13, 106. doi:10.1186/s12916-015-0314-7
- Lucht/Bredenkamp/Boeker/Kramer, 2015. Gesundheits- und Versorgungs-Apps. Hintergründe zu deren Entwicklung und Einsatz. Studie des Universitätsklinikums Freiburg im Auftrag der Techniker Krankenkasse.
- Murakami, H., Kawakami, R., Nakae, S., Nakata, Y., Ishikawa-Takata, K., Tanaka, S., Miyachi, M., 2016. Accuracy of Wearable Devices for Estimating Total Energy Expenditure: Comparison with Metabolic Chamber and Doubly Labeled Water Method. JAMA Intern. Med. 176, 702-703.
- Plante, T.B., Urrea, B., MacFarlane, Z.T., Blumenthal, R.S., Miller, E.R., Appel, L.J., Martin, S.S., 2016. Validation of the instant blood pressure smartphone app. JAMA Intern. Med. 176, 700-702.
- Wolf, J.A., Moreau, J.F., Akilov, O., Patton, T., English, J.C., Ho, J., Ferris, L.K., 2013. Diagnostic inaccuracy of smartphone applications for melanoma detection. JAMA Dermatol. 149, 422-426.