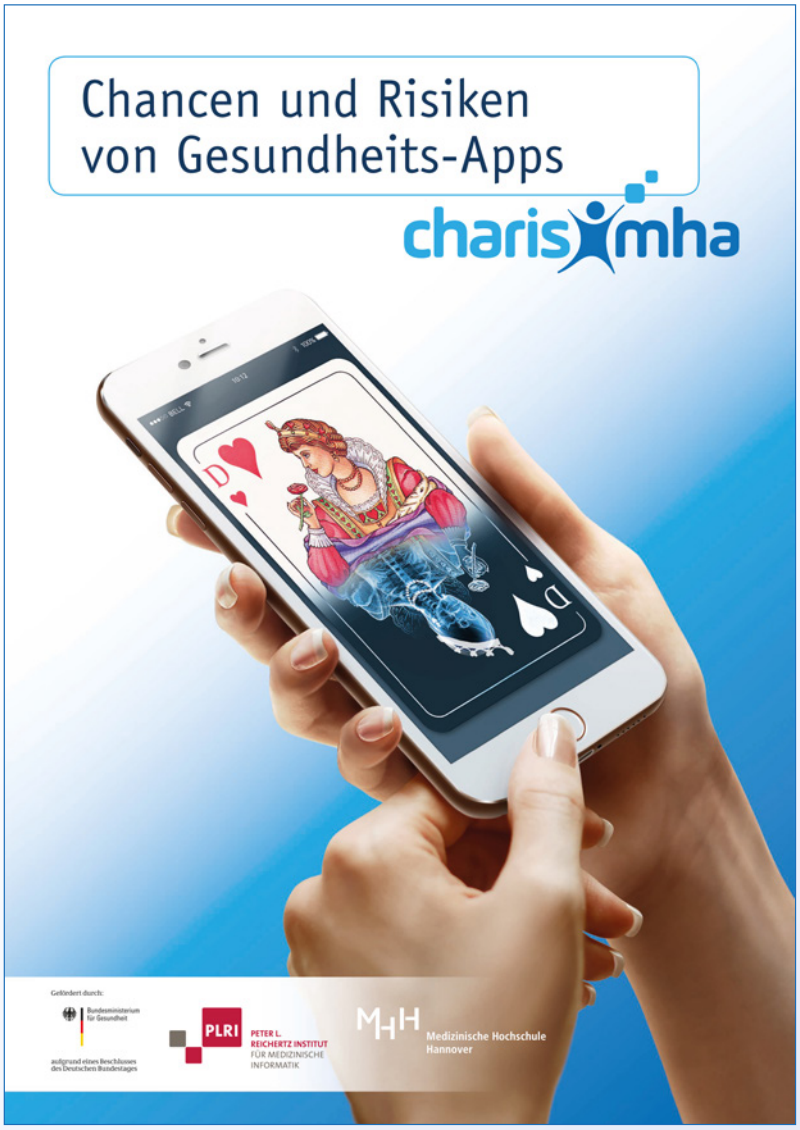
Kapitel 8 Gesundheits-Apps und Risiken

Urs-Vito Albrecht

www.charismha.de

aus:



Zitieren als:
Albrecht, U.-V.: Kapitel 8. Gesundheits-Apps und Risiken.
In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA).
Medizinische Hochschule Hannover, 2016, S. 176–192. urn:nbn:de:gbv:084-16040811340.
http://www.digibib.tu-bs.de/?docid=60014

Version: V.01.3 - 20160424

Kapitel 8

Gesundheits-Apps und Risiken

Urs-Vito Albrecht

Zitieren als:
Albrecht, U.-V.: Kapitel 8. Gesundheits-Apps und Risiken. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 176–192. urn:nbn:de:gbv:084-16040811340. http://www.digibib.tu-bs.de/?docid=60014

1 Ziel

Das Ziel des vorliegenden Kapitels ist die Identifikation von möglichen Gefährdungen und Risiken für die Nutzerinnen und Nutzer von Apps im Gesundheitskontext. Hierzu werden zunächst der Risiko- sowie Schadensbegriff erörtert. Im Zentrum stehen an dieser Stelle insbesondere technische Risiken, die zu Schäden gesundheitlicher Natur, aber auch in Bezug auf den persönlichen Lebensbereich der Anwender sowie ihr Umfeld, führen können. Ethische Risiken werden hingegen an anderer Stelle (s. Kapitel 9) ausführlicher behandelt.

2 Einführung

Die führenden Konzerne verabreden in Verträgen mit den jeweiligen Entwicklern und Nutznießern des Vertriebs, Apps aus ihrem Angebot zu entfernen, die eine ernsthafte Gefahr für die Geräte der Anwenderinnen und Anwender oder ihre Daten bedeuten könnten. Die Angaben dazu, woraus sich solche Gefahren in den Augen der Konzerne ergeben, sind jedoch meist wenig konkret. So spezifiziert Google beispielsweise in seinen Vereinbarungen für den Entwicklervertrieb (Google 2015), dass „keine Handlungen einschließlich der Entwicklung und des Vertriebs von Produkten […]“ vorgenommen werden dürfen, „[…] durch welche Geräte, Server, Netzwerke oder sonstiges Eigentum oder sonstige Dienstleistungen von Dritten beeinträchtigt, gestört oder beschädigt werden oder auf sie in unerlaubter Weise zugegriffen wird.“. Auch bei anderen Plattformen sind die Definitionen ähnlich unscharf: so gibt Apple in seinen App Store Review Guidelines (Apple 2015) neben Design-Richtlinien sowie erwünschten oder nicht-erwünschten Inhalten u.a. Hinweise, dass Apps, die eine Gefahr für das Gerät bedeuten oder körperlichen Schaden verursachen können, nicht zugelassen seien[1] Seitens der Konzerne bleibt jedoch oft unklar, wie sie die Begriffe „Schaden“ oder „Gefahr“, „Risiko“ oder „Chance“ definieren oder was als „körperlicher Schaden“ gewertet wird bzw. welche Maßnahmen zur Prävention und Abwehr getroffen werden (sollen) (s. auch Wetter 2015).

3 Problemstellung

Die Anwendung und auch das Unterlassen der Anwendung von Maßnahmen im Gesundheitskontext beinhalten grundsätzlich neben allen Chancen ein Schadenspotenzial für den Empfänger bzw. die Empfängerin der Maßnahmen. Bei einer wirksamen Maßnahme kann beim Empfänger unabhängig von seinem Gesundheitszustand eine Wirkung nachgewiesen werden, die bei einer unwirksamen Maßnahme hingegen ausbleibt. Beides kann nachhaltige Konsequenzen im Sinne eines Schadens für den Gesundheitszustand des Empfängers mit sich bringen, insbesondere, wenn es sich um eine erkrankte Person handelt. Gesundheits-Apps, deren Anwendung ebenfalls als eine „Maßnahme im Gesundheitskontext“ verstanden werden muss, ist ebenfalls ein solches potenzielles Schadenspotenzial zuzuweisen. Es stellen sich allerdings gleich mehrere Fragen, und zwar, welche Schäden und Gefährdungen hierunter gefasst werden und welche Risiken sich hieraus für die Nutzerinnen und Nutzer ableiten lassen.

[1] „Apps that encourage users to use an Apple Device in a way that may cause damage to the device will be rejected“ und „Apps whose use may result in physical harm may be rejected“.

4 Schaden, Gefährdung und Risiko – Begriffsnäherungen

4.1 Schaden

Schaden

Nach Grimm (Grimm und Grimm 1854) wird „jede Verletzung der Person oder des Eigentums“ als „Schaden“ bezeichnet, auch wenn diese „in der Achtung oder Sympathie der Leute“ herabgesetzt wird. Unter der umfassenden WHO Definition von Gesundheit lässt sich diese Definition gut auf den Gesundheits-Kontext übertragen. Während die soziale Komponente im deutschen Strafrecht im Straftatbestand der Beleidigung mit dem Schutzgut der Ehre (Fischer 2015, Vorbemerkungen zu §§ 185 bis 200, Rn. 1) abgebildet wird, werden gesundheitsbezogene Schäden in Gesundheitsschäden und Schäden der körperlichen Unversehrtheit differenziert (Fischer 2015, § 223, Rn. 2). Die körperliche Unversehrtheit unterscheidet unmittelbare körperliche Schäden („körperliche Unversehrtheit“) und Störungen des körperlichen Wohlbefindens (Fischer 2015, § 223, Rn. 6, 7, m.w.N.). Das körperliche Wohlbefinden stellt dabei den Zustand des Körperempfindens dar, wobei bei einer möglichen Verletzung das somatische und psycho-vegetative Körperempfinden beeinträchtigt sein kann, Angst und Ekel genügen nicht (Fischer 2015, § 223, Rn. 6). Die körperliche Unversehrtheit betrifft die körperliche Integrität und somatische Funktionsfähigkeit. Gleichwohl wird das rein seelische Wohlbefinden nur dann berücksichtigt, wenn somatisch objektivierbare pathologische Zustände hieraus resultieren. Grundsätzlich gilt, dass Schäden in unterschiedlicher Form durch die Anwendung von Gesundheits-Apps kausal verursacht werden können. Zu untersuchen ist daher im Folgenden, auf welche Weise und mit welcher Gefährdungsintensität Gesundheits-Apps mittel- respektive unmittelbar Schäden verursachen können oder diese zur Schadensverursachung eingesetzt werden. Die nachfolgende Untersuchung stellt die potenziellen Verletzungen der Gesundheit, des Körpers sowie des Persönlichkeitsrechts in den Fokus, weil insbesondere hier der Gesundheitsbezug auszumachen ist.

Gesundheitsschäden, Schäden der körperlichen Unversehrtheit

4.2 Gefahr und Gefährdung

Gefahr

Eine „Gefahr“ ergibt sich aus einem großen und ein akzeptables Maß übersteigenden Risikos für den Eintritt eines Schadens (Deutscher Bundestag 1996, S. 16). Im gesundheitlichen Kontext können somit zu einer Gefahr potenziell alle Faktoren beitragen, die zu gesundheitlichen Beeinträchtigungen, gleich welcher Art, führen können. Eine „Gefährdung“ durch Apps im Sinne der Möglichkeit, dass sich eine solche gesundheitliche Gefahr realisiert, ergibt sich aus dem Zusammentreffen der App als einer potenziellen Gefahrenquelle mit einer Person bzw. einem im Gesundheitskontext zu schützenden Objekt, die dabei einen Schaden erleiden können (s. Abschnitt 4.1). Der Begriff der „Gefährdung“ ist dabei unabhängig vom Ausmaß respektive der Eintrittswahrscheinlichkeit (s. Risiko) eines möglichen Schadens (Deutscher Bundestag 1996, S. 16).

Gefährdung

4.3 Risiko

Der Risikobegriff führt das Ausmaß und die Schwere eines durch eine Gefährdung potenziell auftretenden Schadens mit der Wahrscheinlichkeit für das Auftreten dieses Schadens zusammen. Ein „Risiko“ kann somit als Produkt der Eintrittswahrscheinlichkeit eines Schadens mit dem möglichen Schadensausmaß gesehen werden (DIN EN ISO 14971:2013-04). Da sich gerade im Bereich Gesundheit häufig weder mögliche Schäden noch die Wahrscheinlichkeit für ihr Auftreten abschließend quantifizieren lassen, kann auch das sich daraus ergebende Risiko selten genau beziffert werden.

Risiko

5 Gefahrenquellen im unmittelbaren Versorgungsprozess

5.1 Fehlfunktion

Fehler

Nach DIN EN ISO 9000 liegt ein „Fehler“ vor, wenn eine vorgegebene Anforderung/Erwartung nicht erfüllt wird. Im technischen Sinn können Fehler einerseits auf zur Verfügung stehenden oder erhobenen Daten und Signalen beruhen, die von Soll-Werten bzw. zulässigen Werten abweichen (Datenfehler), es kann sich aber auch um Fehler handeln, die aufgrund von Verarbeitungsschritten

und gespeicherten fehlerhaften Ergebnissen (Zustandsfehler) oder darauf basierenden fehlerhaften Ausgaben (Ausgabefehler) zustande kommen (Kemnitz 2007). Eine Fehlfunktion kann nach Kemnitz (2007) als eine „einzelne falsche Ausgabe oder eine durch einen Zustandsfehler verursachte Folge von Ausgabefehlern“ beschrieben werden. Fehlfunktionen können unter anderem durch technische Defekte verursacht werden, aber auch aufgrund von Design-, Konstruktions- und Entwicklungsfehlern auftreten.

Fehlfunktion

5.2 Fehlgebrauch

Selbst wenn das jeweilige Produkt im eigentlichen Sinne fehlerfrei funktioniert, kann es aufgrund unterschiedlicher Faktoren zu Fehlern bei seinem Gebrauch kommen. Israelski und Muto (2012, S. 477) definieren beispielsweise „Gebrauchsfehler“ („use errors“) als einem Muster folgende und vorhersagbare Fehler, die durch unzureichendes oder unsachgemäßes Design verursacht werden[2].

Fehlgebrauch

Wird von einem Fehlgebrauch gesprochen, wird vermieden, die Schuld nur der jeweils anwendenden Person zuzuweisen („menschlicher Fehler“); vielmehr wird zusätzlich auch das jeweilige System, insbesondere auch dessen Design als beteiligter Faktor gesehen (Hörmann 2015). Gründe für einen Fehlgebrauch können somit – neben solchen, die tatsächlich in der Verantwortung der jeweiligen Person liegen (z.B. Übermüdung, Unachtsamkeit) – viele Faktoren einschließen (Israelski und Muto 2012, S. 477):

- schlechtes Design der Bedienoberfläche und damit schlechte Gebrauchstauglichkeit,
- organisationsbedingte Probleme, z.B. mangelnde Ausbildung bzgl. des Gebrauchs oder fehlende Unterstützungsangebote,
- fehlende Berücksichtigung der Umgebungsbedingungen, unter denen der Einsatz erfolgt,
- mangelndes Verständnis der Entwickler für die üblichen Aufgaben und Aufgabenabläufe der Nutzerinnen und Nutzer,
- fehlendes Verständnis bzgl. der Vorkenntnisse und Erfahrungen der Anwenderinnen und Anwender sowie ihrer Motivation.

5.3 Fehlinformationen

Fehlinformation

Information, die nicht verlässlich, überholt, unverständlich oder dem Zweck unangemessen ist, kann zu weitreichenden Konsequenzen für die Gesundheit der (Versorgungs-) Empfangenden führen. Die Information wird in der Regel als Grundlage für Entscheidungsprozesse genutzt, die unmittelbar mit Gesundheit in Beziehung stehen, sei es bei Fragen der Gesundheitsförderung oder Prävention, aber noch gravierender bei Diagnostik und Therapie. Auf fehlerhaften, unzureichend validierten, unvollständigen oder unverständlichen Informationen beruhende Fehlentscheidungen können sich einerseits bei einer Anwendung durch Dritte (Ärzte, andere Heilberufe) mittelbar auswirken, andererseits in der eigenen Anwendung durch die betroffenen Nutzer aber auch unmittelbare Konsequenzen mit sich bringen.

5.4 Fehldiagnostik

Mit Stellung der Diagnose wird in der Regel ein Zustand oder eine Erkrankung benannt. Dabei kann es sich auch um mehrere Verdachts- und/oder Differenzialdiagnosen handeln. Die damit verbundenen Erkenntnisse, zusammen mit dem aktuellen Gesundheitszustand und den vorherrschenden Rahmenbedingungen, führen zur Therapieentscheidung und Durchführung von Maßnahmen. Eine Fehldiagnostik kann somit zu weitreichenden Konsequenzen für die Gesundheit der Patientin oder des Patienten führen, insbesondere wenn eine Behandlung einsetzt, die nicht für das vorliegende Erkrankungsbild geeignet ist.

Fehldiagnostik

Fehldiagnostik liegt vor, wenn

- ein Zustand/eine Erkrankung nicht erkannt wird, obwohl er/sie existiert,
- ein Zustand/eine Erkrankung in ihrer Schwere falsch interpretiert wird,
- ein Zustand/eine Erkrankung falsch erkannt wird,
- ein Zustand/eine Erkrankung in der Verlaufsentwicklung falsch interpretiert wird.

[2] „Use errors are defined as a pattern of predictable human errors that can be attributable to inadequate or improper design.“

5.5 Fehlbehandlung

Die Wahl der geeigneten Therapie und deren Durchführung hängen von vielfältigen Faktoren ab. Es müssen hier auch individuelle Aspekte der Empfängerinnen und Empfänger berücksichtigt werden. Nicht jede Maßnahme ist gleichermaßen für alle Patienten geeignet; die Entscheidung muss, auch wenn es um den Einsatz von Apps im therapeutischen Kontext geht, stets unter Einbeziehungen der individuellen Umstände fallen. Die Abwägung von Risiken und Nutzen sollte von Behandelnden bzw. Anwendern unter Berücksichtigung der Diagnose, der psychischen und physischen Ressourcen der Empfängerin/des Empfängers sowie der eigenen Fähigkeiten und Kenntnisse unter den gegebenen Rahmenbedingungen (Verfügbarkeit der Mittel) getroffen werden. Konkrete Risiken können sich in allen Stadien der Therapie, von deren Planung bis zu ihrer Durchführung, ergeben. Wird eine ungeeignete Therapie oder eine geeignete Therapie nicht adäquat angewendet, führt dies selten zu einer Verbesserung des Zustands des Empfängers oder seiner Erkrankung. Im Falle der Anwendung einer ungeeigneten Therapie kommt es nicht nur zu einem Ausbleiben des Behandlungserfolgs, sondern auch zu einer zusätzlichen und vermeidbaren Belastung des Körpers, die je nach Wirksamkeit der therapeutischen Maßnahme auch eine deutliche Verschlimmerung bedeuten kann. Auch die verzögerte oder beschleunigte Anwendung einer geeigneten Therapie kann negative Auswirkungen auf den Krankheitsverlauf und den aktuellen Zustand des Empfängers haben.

Fehlbehandlung

Fehlbehandlung liegt vor, wenn

- eine nicht dem Zustand/der Erkrankung entsprechende, daher hierfür ungeeignete Therapie angewendet wird (falsche Therapie),
- eine dem Zustand/der Erkrankung entsprechende Therapie im nicht genügend wirksamen Regimen durchgeführt wird (Unterdosierung, Unteranwendung),
- eine dem Zustand/der Erkrankung entsprechende Therapie in überwirksamen Regimen durchgeführt wird (Überdosierung, Überanwendung).

5.6 Datenmissbrauch

Datenmissbrauch

Je mehr Informationen über eine Person vorliegen, desto einfacher ist der Rückschluss auf deren Identität, selbst wenn diese verstreut und ohne offensichtlichen Bezug vorliegen. Durch die immer dichter werdende Vernetzung, den erhöhten Datenanfall aus unterschiedlichsten Quellen und die Steigerung der Rechenleistung der beteiligten Systeme gelingt das Finden und Kombinieren von Information effizienter. Insbesondere das Einstellen sensibler Gesundheitsinformationen und etwaiger genetischer Informationen (z.B. im Zusammenhang mit eigenen Bemühungen in der Ahnenforschung) steigert das Risiko der eigenen Identifizierung, aber auch der des (unbeteiligten) sozialen Umfeldes aus Familie, Freunden, Bekannten und sogar Fremden, wenn sie im Sinne einer Schicksalsgemeinschaft (z.B. Krankenhausaufenthalt auf derselben Station) mit dem Bereitsteller der Information in Verbindung gebracht werden können. Ebenso lassen sich durch eine Übermittlung von Standort- und Bewegungsdaten beispielsweise leicht detaillierte Bewegungsprofile erstellen oder Gewohnheiten ermitteln und – unter Einbezug weiterer Informationen – auch die Risikofreudigkeit bei Freizeitaktivitäten oder ähnliches erkennen; auch die Inanspruchnahme bestimmter (Gesundheits-) Dienstleistungen kann hierüber hergeleitet werden. Solche Daten sind sicherlich auch für Dritte, wie beispielsweise Versicherungen von Interesse, die sie zur Ermittlung risikoadaptierter Tarife nutzen könnten (sei es um Versicherten einen Rabatt zu gewähren oder gesundheitsschädliches Verhalten zu sanktionieren), worauf Kapitel 12 noch näher eingeht. Risiken wirtschaftlicher Natur können sich hierbei beispielsweise für bestimmte Gruppierungen ergeben, bei denen Risiken bestehen, die sie nicht selbst steuern können, z.B. im Falle chronischer Erkrankungen oder körperlicher Gebrechen.

6 Schäden durch Software in Medizinprodukten

Schäden durch Gesundheits-Apps werden nur selten berichtet

Die Ermittlung von tatsächlich eingetretenen Schäden durch Gesundheits-Apps ist schwierig, da die Literatur hierzu wenig aussagekräftig ist. Oftmals finden sich lediglich Hinweise in der Presse, die über Fälle berichtet, deren Validität aber regelmäßig nicht durch eine wissenschaftliche und rechtliche Aufarbeitung belegt wird. Zusätzlich werden vereinzelt Rückrufe seitens der Hersteller publik, sofern Probleme festgestellt wurden (z.B. Pfizer 2011, BfArM 2011). Aufgrund

des für Medizinprodukte-Software und -Geräte bestehenden Vigilanzsystems sind konkrete Fälle dokumentiert bei denen Patienten zu Schaden kamen (z.B. Leveson und Turner 1993; fehlerhafte Software bei einem zur Strahlentherapie genutzten Linearbeschleuniger verursachte massive Verstrahlungen), die allerdings nur im Sinne der Analogie verwendet werden können (s. auch 1). Vielfach werden in diesem Kontext auch Risiken bezüglich Datenschutz und Datensicherheit aufgezeigt bzw. deren (potenzielle) Auswirkungen (Paul, Kohno und Klonoff 2011), aber auch Möglichkeiten zur Verringerung der Risiken beschrieben (Fu und Blum 2014, Kramer et al. 2012).

Tabelle 1: Beispiele von Schäden durch Software in Medizinprodukten, erweitert nach (Fu 2011).

Entwicklungsphase / Teilaspekt	Ausgelöster Schaden bzw. Potenzial dafür	Beitragende Faktoren und Beispiele
Spezifikationsphase und Design	Patienten/Patientinnen wurden durch fehlerhafte Software und zudem fehlende Schutzmechanismen in einem zur Strahlentherapie genutzten Linearbeschleuniger verstrahlt und starben. (Leveson und Turner 1993, Leveson 1995).	Zu bemängeln war die nicht ausreichende Dokumentation bzgl. der Spezifikation und Testung der Software sowie unzureichendes Systemdesign ohne (hard- und/oder softwarebasierte) Sicherheitssperren bei bestimmten Fehlerzuständen (Leveson 1995).
Menschlicher Einfluss	Infusionspumpen schaden Patienten/Patientinnen durch Verabreichung einer falschen (zu hohen) Medikamentendosis bzw. zu rasche oder zu langsame Verabreichung des Medikaments.	Software führt keine Plausibilitätsprüfung durch, ob durch das Prellverhalten mechanischer Taster Fehleingaben entstehen, so wurden 20 mL als 200 mL interpretiert (Flournoy 2010). Infusionspumpe verabreicht ein Medikament nach Fehleingabe innerhalb von 20 Minuten statt 20 Stunden (Fu 2011).
Implementierung	Infusionspumpe verabreicht eine zu geringe Dosis eines Medikaments, wodurch der Hirndruck eines Patienten stieg, es kam zum Hirntod.	Die Pumpe stellte den Betrieb aufgrund eines Programmierfehlers ein (Pufferüberlauf).
Testen	Problem in Rettungsleitstellen durch neue Software: Notrufe konnten nicht bearbeitet werden oder gingen verloren.	Ungenügende Tests und Nichtbeachtung grundlegender Anforderungen an die Entwicklung ließen Probleme erst im laufenden Betrieb offensichtlich werden: U.a. kam es zu Inkonsistenzen in der Datenbank der Verwaltungssoftware, wodurch die Position von Rettungsfahrzeugen oft unbekannt war und Ressourcen nicht korrekt eingesetzt werden konnten.
Wartung / Instandhaltung	Gesundheitsinformationssysteme bzw. -Geräte verlieren durch fehlerhafte Updates oder Cyberattacken ihre Funktionsfähigkeit; dies muss nicht zwingend in dem jeweiligen Produkt selbst begründet sein.	Antivirensoftware klassifizierte nach einem fehlerhaften Update Komponenten des Betriebssystems oder der Software des Informationssystems als potenziellen Schädling und verschob die jeweiligen Komponenten in eine Quarantäne. Das System wurde dadurch außer Betrieb gesetzt und ließ sich nicht mehr starten (Spiegel Online 2010). Betroffen waren auch Krankenhäuser (syracuse.com 2010).

7 Gefahren durch Gesundheits-Apps

7.1 Beeinflussung der körperlichen Unversehrtheit

7.1.1 Fehlfunktion

Fehlfunktion

Diverse Quellen beschreiben gesundheitsbezogene Gefahren oder datenschutzbetreffende Gefahren durch Apps und betriebene Technik, jedoch ohne den Beleg konkreter Schadensfälle (z.B. Papadopoulos, Pappa und Gortzis 2006, Papadopoulos, Pappa und Gortzis 2007, Giota und Kleftaras 2014, Mare und Kotz 2010). Hierbei handelt es sich zuvorderst um technische Probleme, wie beispielsweise fehlerhafte Netzteile oder (Drittanbieter-) Akkus, die zu einer Überhitzung oder gar Explosion der Geräte und somit auch potenziell zu Verbrennungen und ähnlichen Verletzungen führen können (CHIP Online 2015).

7.1.2 Fehlgebrauch

Fehlgebrauch

Mittelbar sind verschiedene Schadensmechanismen beim Einsatz mobiler Apps denkbar, die auf die körperliche Unversehrtheit der Anwenderinnen und Anwender bzw. der ihnen anvertrauten Personen wirken können. Hierzu zählen indirekt auch Hygiene-Aspekte bei der Nutzung mobiler Lösungen, die in diesem Zusammenhang zu bedenken sind: Mobile Geräte können beispielsweise, wenn sie bei vulnerablen Patientinnen und Patienten (z.B. mit beeinträchtigtem Immunsystem) eingesetzt werden, als potenzieller Vektor für die Übertragung von (möglicherweise multiresistenten) Erregern fungieren (Walia et al. 2014), die die Gesundheit und das Leben dieser Patienten gefährden können; insbesondere beim Einsatz mHealth-basierter Lösungen im professionellen Umfeld sollte daher, wie auch beim Umgang mit anderen Gerätschaften, stets auf ausreichende Hygiene geachtet werden (Albrecht et al. 2013).

7.1.3 Fehldiagnostik

Fehldiagnostik

Bei einem Einsatz zu Diagnosezwecken kann es durch eine Fehldiagnose zur verzögerten Zuführung zur adäquaten Therapie kommen. Als Beispiel seien hier Apps für den Bereich Dermatologie genannt, deren Ziel ist es, verdächtige Stellen auf der Hautoberfläche hinsichtlich ihrer potenziellen Bösartigkeit zu untersuchen. Bereits 2013 wurde in einer Studie von Wolf et al. (Wolf et al. 2013), in der mehrere entsprechende Smartphone-Apps evaluiert wurden, festgestellt, dass viele Apps hinsichtlich Spezifität und Sensitivität nur unbefriedigende Resultate erbringen; die Ergebnisse wurden später auch von anderen Autoren in ähnlicher Weise bestätigt (Kassianos et al. 2015). Die unzureichende Erkennungsrate mag auch auf den unterschiedlichen Eigenschaften der genutzten Smartphone-Kameras bzw. der fehlenden Standardisierung hinsichtlich der Aufnahmebedingungen gründen; die per Smartphone-Kamera aufgezeichneten Bilddaten erreichen somit oft weder hinsichtlich der Auflösung noch sonstiger Qualitätskriterien die im klinischen Bereich nötigen Anforderungen (Ali 2015). Gibt eine solche App fälschlicherweise Entwarnung, die anwendende Person verlässt sich auf die Aussage der App und nimmt nicht den eigentlich angeratenen Kontakt mit einem Arzt oder einer Ärztin auf, wird auch die nötige zeitnahe Einleitung weiterführender Diagnostik und Therapie verzögert, was gerade bei schwarzem Hautkrebs (malignes Melanom) die zunächst noch mögliche Heilung erschweren oder verhindern kann.

7.1.4 Fehlbehandlung

Fehlbehandlung/ Fehldosierungen

Weitere Schadpotenziale bergen Apps, die zu einer Fehldosierung von Medikamenten beitragen können. Berechnen Apps z.B. aufgrund der erfassten Daten einer Diabetikerin oder eines Diabetikers, basierend auf Blutzuckermesswerten bis hin zur angegebenen Kohlenhydrataufnahme beispielsweise eine zu verabreichende Insulindosis falsch, kann es zu einer potenziell bedrohlichen Hypoglykämie kommen. In einer von Huckvale et al. durchgeführten Studie, in der 46 entsprechende Apps untersucht wurden (Huckvale et al. 2015a), konnten bei immerhin 31 Apps Probleme festgestellt werden, die von der Verletzung üblicher klinischer Standards bei der Berechnung bis hin zu Problemen bei der Umsetzung selbst reichten (Fehler bei der Berechnungsformel, ungenügende Plausibilitätschecks bei der Eingabe). Entsprechende Probleme wurden auch von anderen Autoren bemängelt (Wicks und Chiauzzi 2015, Bierbrier, Lo und Wu 2014). Bei der mit iOS 8.2 bereitgestellten Health App konnten Blutzuckerwerte manuell zunächst nur wie z.B. in den USA

üblich als mg/dL erfasst und angezeigt werden, für die in vielen anderen Ländern gebräuchliche Einheit mmol/L funktionierte die manuelle Eingabe anfänglich nicht (Ben 2014). Für konkrete Schäden, die hierdurch verursacht wurden, fanden sich allerdings keine Hinweise.

Im Zusammenspiel von Apps mit anderen Medizinprodukten, wie beispielsweise Insulinpumpen, kann es ebenfalls zu Problemen kommen, die sowohl durch Probleme innerhalb einer App bzw. dem angesteuerten Medizinprodukt selbst bedingt sein als auch durch die Kommunikation zwischen der auf dem Mobilgerät laufenden App und dem jeweiligen Medizinprodukt verursacht werden können. Wird die Kommunikation aufgrund technischer Mängel gestört oder ist sie nicht ausreichend vor Eingriffen von außen geschützt, kann es hierdurch wiederum zu Fehldosierungen oder anderen Fehlsteuerungen kommen, die gesundheitliche Konsequenzen haben und somit die körperliche Integrität gefährden: Beispielsweise könnte die über eine Insulin-Pumpe verabreichte Dosis hierdurch beeinflusst werden (Radcliffe 2011).

7.1.5 Fehlbelastungen

Fehlbelastungen bei der Nutzung mobiler Geräte

Gefährdungen können sich aus einer übermäßigen Nutzung mobiler Geräte und Apps im täglichen Umgang ergeben: genannt werden hier insbesondere Überlastungen der oberen Extremitäten und die sich daraus ergebenden Konsequenzen (z.B. Tendinosen, Sharan et al. 2014; Beeinträchtigung des Nervus medianus, Inal et al. 2015; „WhatsAppitis“ im Sinne einer Tendinitis durch kontinuierliche Nutzung einer Nachrichten-App (Fernandez-Guerrero 2014). Für eine direkte Assoziation entsprechender Schäden mit der Nutzung von Apps im Gesundheitskontext fanden sich in der Literatur jedoch keine Hinweise, obwohl sie bei exzessiver Nutzung möglicherweise einen – wenn auch vermutlich geringen – Beitrag dazu leisten könnten.

7.1.6 Einflüsse durch elektromagnetische Strahlung

Einflüsse elektromagnetischer Strahlung auf Anwenderinnen und Anwender und ihre Umgebung

In der Literatur wird kontrovers diskutiert, ob die im Zusammenhang mit der Nutzung von Mobiltelefonen auftretende Strahlung (Paffi et al. 2015) negative Auswirkungen auf verschiedene Gewebetypen des menschlichen Körpers hat und somit ein erhöhtes Risiko für das Auftreten bestimmter Tumoren mit sich bringt, z.B. im Bereich des Kopfes (z.B. Meningiome oder Akustikusneurinome). In einer Review-Arbeit zu diesem Themenkomplex fanden Repacholi et al. (2012) keine signifikanten Hinweise hierauf, gaben aber zu bedenken, dass die Langzeiteffekte noch nicht ausreichend erforscht seien. Auch Vermutungen, dass eine intensive Nutzung von Mobiltelefonen das Auftreten von Hautkrebs begünstigen könne, ließen sich in der Literatur nicht bestätigen (Poulsen et. al. 2013).

Bezüglich der vorgenannten Aspekte steht jedoch sicherlich die Nutzung mobiler Geräte im alltäglichen Gebrauch im Vordergrund; ein entsprechendes, speziell durch die Nutzung von gesundheitsbezogenen Apps bedingtes Risiko wird eher zu vernachlässigen sein.

Hingegen sind durchaus Einflüsse auf sensible und teils lebenswichtige Medizingeräte zu beobachten, die im alltäglichen Umgang mit den mobilen Geräten (und somit auch beim Umgang mit gesundheitsbezogenen Apps) berücksichtigt werden müssen. Ein Beispiel hierfür sind implantierbare Herzschrittmacher, deren Elektroden (die einerseits dem Erfassen der Herzaktivität, aber auch der Abgabe der Schrittmacher-Impulse dienen) im ungünstigen Fall als eine „Antenne“ für die vom Mobiltelefon abgegebene elektromagnetische Strahlung wirken können. Hierdurch kann die Funktion des Schrittmachers potenziell beeinträchtigt werden, obwohl viele moderne Schrittmacher die Einflüsse entsprechender Frequenzen meist durch technische Maßnahmen, d.h. über Filter, zu minimieren suchen (Endo et al. 2013); dennoch verbleibt ein Restrisiko.

7.2 Beeinflussung des körperlichen Wohlbefindens

Einfluss auf das körperliche Wohlbefinden

Abhängig vom jeweiligen Anwendungsfall und der Präsentation bestimmter Reize innerhalb einer App ist auch bei Nutzung mobiler Smart-Devices und darauf laufender gesundheitsbezogener Apps eine Beeinflussung des körperlichen Wohlbefindens denkbar.

In der Literatur finden sich Hinweise für das mögliche Auftreten einer sog. „Cybersickness“ bei dafür empfänglichen Personen, z.B. bei Anwendungen aus dem Bereich der virtuellen (VR) respektive augmentierten Realität (AR) (Kiryu und So 2007, Nalivaiko et al. 2015), bei denen der Nutzende in eine virtuelle Realität eintaucht bzw. ihr oder ihm zusätzliche (meist visuelle) Inhalte in eine

Abbildung der Realität eingeblendet werden. Die Auswirkungen dieser Cybersickness können in etwa denen der Reisekrankheit entsprechen und von Schwindelgefühlen und Kaltschweißigkeit sowie erhöhter Herzfrequenz bis hin zu Übelkeit und im Extremfall Erbrechen reichen. Auslöser können z.B. kurze Verzögerungen (Latenzen) zwischen der Kopfbewegung des Anwenders und der Anpassung der im Display dargestellten Position in der virtuellen Umgebung sein; denkbar sind aber auch Einflüsse durch hochfrequentes Flackern oder eine zu rasche Änderung der dargestellten Inhalte. In der Literatur sind keine direkten Hinweise auf das Auslösen entsprechender Effekte durch Gesundheits-Apps beschrieben. Es finden sich in diesem Bereich, von der Ausbildung bis hin zu Apps mit therapeutischem Anspruch, jedoch zunehmend auch Smartphone-basierte VR- und AR-Anwendungen (Guze 2015, Mosso et al. 2009) und entsprechende Effekte sind somit auch hier denkbar. In der Presse wird das Problem der „Cybersickness" teils auch bereits als durch dreidimensionale Designelemente auslösbar beschrieben (Antony 2013).

7.3 Beeinflussung des seelischen Wohlbefindens

Einfluss auf das seelische Wohlbefinden

Negative Auswirkungen des Gebrauchs von Gesundheits-Apps sind beispielsweise durch das unbeabsichtigte Auslösen oder Verstärken von – berechtigten wie unberechtigten – Ängsten bzgl. der eigenen Gesundheit durch in den Apps bereitgestellte Informationen und Funktionen zu erwarten. Gefahren ergeben sich hier potenziell – wie auch bei anderen digitalen Technologien (Starevic und Aboujoude 2015) – durch eine exzessive Nutzung der Technologie. Dem übermäßigen Gebrauch von Smartphones und Apps wird auch das Potenzial zugesprochen, als ein Auslöser für Depressionen sowie Schlaf- und Angststörungen zu wirken (Demirci, Akgönül und Akpinar 2015) bzw. Suchtverhalten auszulösen, ähnlich wie dies bereits seit längerem für die Nutzung anderer digitaler Angebote, insbesondere aus dem Online-Bereich, beschrieben wird (Kuss und Griffiths 2011, Kuss und Griffiths 2012). Denkbar ist (obwohl nicht explizit dargestellt), dass auch gesundheitsbezogene Apps einen zusätzlichen Beitrag zu diesen Problemen leisten und somit negativen Einfluss auf das seelische Wohlbefinden nehmen können.

Vielen Nutzerinnen und Nutzern gelingt es zudem auch bei Gesundheits-Apps nicht, zwischen glaubwürdigen und eher zweifelhaften Quellen und Inhalten zu unterscheiden oder es mangelt an der Fähigkeit, die dargebotenen Informationen korrekt zu interpretieren, was ebenfalls einen negativen Einfluss auf die Wahrnehmung mit Bezug zur eigenen Gesundheit haben oder unrealistische Erwartungen an die Funktionalitäten einer App auslösen kann; ein Problem, das auch für über das Internet recherchierte Informationen gilt (Fergus 2013).

Insbesondere bei solchen Apps, die eine Interaktion und Kommunikation mit anderen erlauben (Parime und Suri 2014), z.B. über Anbindung sozialer Medien oder Foren, kann es zudem zu Cybermobbing oder Konflikten kommen, wie es generell auch bei internetbasierten Anwendungen (Starevic und Aboujoude 2015) möglich ist; vulnerable Gruppen wie Jugendliche oder psychisch Erkrankte sind hier auch im sensiblen Bereich der Gesundheit als besonders gefährdet zu sehen.

Zudem ist denkbar, dass Apps, die Inhalte unangemessen zur Darstellung bringen oder schlechte Handhabungseigenschaften besitzen, Stress verursachen können.

7.4 Missachtung der Persönlichkeitsrechte

Eine Missachtung der Persönlichkeitsrechte kann auf vielfältige Weise geschehen

Apps können durch beabsichtigte wie unbeabsichtigte Verletzungen grundlegender Datenschutz- und Datensicherheitsgrundsätze die Persönlichkeitsrechte ihrer Anwender verletzen, z.B. indem persönliche (Gesundheits-) Informationen ohne deren Zustimmung nicht-autorisierten Dritten oder der Öffentlichkeit zugänglich gemacht werden[3]; Schäden können hier beispielsweise durch Nutzung dieser Informationen zu Zwecken entstehen, die nicht im Sinne derer sind, auf die sich die Daten beziehen. In einem 2015 von ePrivacy publizierten Whitepaper (ePrivacy GmbH 2015) zu Datenschutz und Datensicherheit gesundheitsbezogener Apps ließen sich bei 80 Prozent der 141 untersuchten Apps die Login-Daten durch unberechtigte Dritte auslesen und somit ein Zugriff

[3] Apps unterlaufen häufig die Kontrollmechanismen der App Stores und geben ungefragt sensible Daten an Dritte weiter oder enthalten Schadcode, der Gefahren für die Anwender und ihre Daten ebenso wie für ihre Geräte birgt. Erst im Oktober 2015 entfernte Apple über 250 Apps, in denen eine integrierte Werbe-Bibliothek für eine – von Entwicklern wie Nutzern unbeabsichtigte – Weitergabe von persönlichen Daten an unberechtigte Dritte gesorgt hatte (Rossignol 2015). Auch für andere Mobilplattformen, z.B. Android, werden immer wieder ähnliche Vorkommnisse bekannt, bei denen Apps mit integriertem Schadcode den Weg in den Store und auf die Geräte der Nutzer finden (Steele 2015).

auf die Daten erlangen. Ebenso wurden die Daten durch mangelnde oder fehlerhaft umgesetzte Verschlüsselung dem Risiko unberechtigten Zugriffs ausgesetzt. Zudem ist häufig das Fehlen, die mangelhafte Verständlichkeit oder unzureichende Umsetzung von Datenschutzerklärungen zu bemängeln. In einer von Sunyaev et al. (2015) vorgestellten Arbeit lag der Anteil der je Plattform analysierten 300 gesundheitsbezogenen Apps, die eine solche Erklärung bereithielten gerade einmal bei 38,3% (iOS) und 22,7% (Android). Bei vorhandenen Datenschutzerklärung fiel auf, dass diese sich häufig nicht auf die jeweilige App selbst, sondern auf unterschiedliche Produkte der Herstellerinnen und Hersteller bezog, teils auch auf die Webseite des Herstellers oder Dienste, mit denen die App in Verbindung stand. Durch die mangelnden Angaben wird eine Beurteilung, ob Persönlichkeitsrechte durch die Hersteller adäquat gewürdigt werden zusätzlich erschwert.

7.4.1 Datenzusammenführung

Datenzusammenführung aus unterschiedlichen Quellen

Problematisch für die Nutzerin oder den Nutzer können nicht nur Big-Data-Ansätze unter reiner Auswertung gesundheitsbezogener Daten sein, die neben dem Verfolgen offensichtlich gesundheitsbezogener Interessen häufig auch dazu dienen, wirtschaftliche Interessen zu stützen (Weber 2015). Eine Nutzung aggregierter Daten kann bereits in kleinerem Maßstab, auf individueller Ebene, Risiken für den Einzelnen bedeuten, ohne dass ihm dies bewusst wird. Werden beispielsweise Online-Dienste in Apps integriert und wird hierfür auf die auf den Geräten installierten Browserkomponenten zurückgegriffen, ergibt sich als zusätzliches Risiko eine Offenbarung der Anwenderinnen und Anwender. Häufig werden beim Aufruf von Webseiten serverseitig neben verwendetem Betriebssystem auch Informationen über den jeweiligen Browser sowie potenziell weitere Konfigurationsmerkmale (installierte Schriftarten, Bildschirmauflösung, Systemfarben etc.) skriptgesteuert ausgelesen und erfasst. Die so erfassten Merkmale können potenziell für die Erstellung eines virtuellen „Fingerabdrucks“ dienen, über den die Nutzerin oder der Nutzer zwar nicht unbedingt namentlich erkennbar, aber dennoch möglicherweise eindeutig identifizierbar wird (Tillmann 2012); ein entsprechender Fingerabdruck wäre auch auf Basis anderer, nicht browserbasierter Daten denkbar. Dies ist gerade auch in gesundheitsbezogenem Einsatzbereich kritisch zu sehen.

7.5 Bewusste Angriffe durch Dritte

Gefahr durch bewusste Angriffe

Drahtlos an Smartphones oder Tablets angebundene Geräte für den Gesundheitsbereich werden häufig nicht nach Sicherheitsgesichtspunkten entwickelt. Dies kann zu Gefährdungen in allen vorgenannten Bereichen führen. Mögliche Angriffsszenarien sind vielfältig. Hier ist u.a. die Möglichkeit eines unberechtigten Abgreifens von Daten oder schlimmstenfalls die Beeinflussung der Steuerungs-App durch zeitgleich auf dem Gerät laufende Software zu nennen. Besonders problematisch können aber auch die Kommunikationskomponenten sein, die für den Datenaustausch zwischen einem Medizinprodukt (Medikamentenpumpen etc.) und App sorgen, z.B. über Bluetooth (Haataja und Hypponen 2008). Die Probleme können hier sowohl durch unzureichende Umsetzung von Sicherungsmaßnahmen in den Apps selbst verursacht werden, als auch indirekt entstehen, z.B. über Einbindung von Komponenten des jeweiligen Betriebssystems. Zwar werden sich die Herstellerinnen und Hersteller zunehmend dieser Problematik bewusst. Dennoch sind viele Geräte vulnerabel und ermöglichen so beispielsweise Man-In-The-Middle-Attacken[4] mit unterschiedlichen gesundheitlichen und sonstigen Folgen für die Anwenderinnen und Anwender (Pournaghshband et al. 2014).

[4] Bei einer Man-in-the-Middle-Attacke (MITM) schaltet sich ein Angreifer entweder physikalisch oder logisch in die Kommunikation zwischen zwei oder mehr Kommunikationspartner. Es ist ihm dabei oft nicht nur möglich, die vollständige Kontrolle über den Datenverkehr zu erlangen und Daten auszulesen. Es lassen sich auf diesem Weg auch übertragene Daten manipulieren. Den Kommunikationspartnern wird dabei nur vorgespiegelt dass die Kommunikation mit dem jeweils erwarteten Gegenüber stattfindet.

Tabelle 2: Mögliche Angriffsszenarien im App-Kontext bei der Datenkommunikation oder durch zusätzlich installierte Apps.

Angriffsszenario	Konsequenz
Unberechtigtes (Mit-) Lesen von medizinischen Daten bereits während der Aufzeichnung.	Verletzung der Privatsphäre, Gesundheitsrisiko.
Abruf gespeicherter Gesundheitsdaten.	Verletzung der Privatsphäre durch Auslesen identifizierender Daten sowie Daten zur Krankengeschichte.
Nicht-autorisierte Steuerung des angebundenen Geräts (Medizinprodukts).	Änderung von Parametern, z.B. einer zu verabreichenden Medikamentendosis, die gravierende Folgen für die Gesundheit hat.
Nicht-autorisierte Änderung der Einstellungen des angebundenen Geräts.	Änderung sicherheitsrelevanter Einstellungen, die zukünftige weitere Angriffe erleichtern.
Komplette Übernahme der Kommunikation durch den Angreifer oder verhindern der Kommunikation des Patienten-Smartphones mit dem zu steuernden Gerät.	Eingreifen des Patienten bei nötigen Anpassungen der Geräteeinstellungen wird erschwert bzw. verhindert, da die nötigen Steuerungskommandos nicht übertragen werden.

8 Szenarien

Es werden exemplarisch einige Szenarien dargestellt. Die Liste erhebt keineswegs den Anspruch auf Vollständigkeit. Auch können die einzelnen Szenarien unter unterschiedlichen Fokussen betrachtet werden. Die Ausprägung der Gefährdung kann je nach individueller psychischer und physischer Ausstattung erheblich variieren.

Tabelle 3: Exemplarische Darstellung von Gefährdungsszenarien.

Körperliche Unversehrtheit	
Szenario	**Mögliche Gefährdung**
• Mobilgeräte-Nutzung durch medizinisches Personal bei der Betreuung von immungeschwächten Patienten.	→ Bei mangelnder Hygiene/fehlenden Desinfektionsmaßnahmen können potenziell gefährliche Erreger von Patient zu Patient weitergegeben werden (Borer et al. 2008, Albrecht et al. 2013).
• Patient verlässt sich auf eine von einer App gestellten Diagnose.	→ Aufnahmen von Leberflecken zur Beurteilung ihrer Bösartigkeit werden fälschlich als harmlos bewertet (Wolf et al. 2013, Kassianos et al. 2015). → Symptomchecker (Semigran et al. 2015) schätzen eine potenziell gefährliche Erkrankung des Hilfesuchenden falsch ein; in der Konsequenz wird zu spät die nötige professionelle medizinische Hilfe gesucht und Diagnostik/Therapie verzögert.
• Therapiebegleitung chronisch Erkrankter.	→ Informationsfehler: Huckvale et al. stellen fest (Huckvale et al. 2015b), dass viele für Asthma-Patienten bereitgestellte Apps inkorrekte bzw. nicht den Richtlinien entsprechende Empfehlungen zum Management der Erkrankung, aber auch bezüglich spezifischer Therapieschritte, z.B. zur Anwendung von Inhalatoren, bereitstellen.

Fortsetzung auf der nächsten Seite

Fortsetzung Tabelle 3

Szenario	Mögliche Gefährdung
• Nutzung einer Smartphone-App durch einen Behandler oder den Betroffenen selbst zur Berechnung von für die Therapie wichtigen Parametern.	→ Dosis eines zu verabreichenden Medikaments wird zu hoch oder zu niedrig angesetzt und der Patient kommt hierdurch zu Schaden. → Apps, die basierend auf Blutzuckermesswerten bis hin zur angegebenen Kohlenhydrataufnahme eine zu verabreichende Insulindosis falsch berechnen, können eine potenziell bedrohliche Hypoglykämie auslösen.
• Nutzung mobiler Geräte und Apps im allgemeinen oder gesundheitsbezogenen Kontext.	→ Von einer Gesundheits-App unabhängige Hard- oder Softwareprobleme des verwendeten Mobilgeräts (z.B. Netzteil, Akku) führen zu gesundheitsgefährdenden Fehlfunktionen. → Denkbare Beeinflussung einer Gesundheits-App durch zu anderen Zwecken installierte Apps oder Schadsoftware
• Einsatz einer ungeeigneten App durch den Patienten bei bestehender, aber noch nicht adäquat diagnostizierter Erkrankung.	→ Nutzung einer einfachen Entspannungs-App bei Posttraumatische Belastungsstörung (PTBS) → Einsatz von Diät-Apps durch Untergewichtige

Körperliches Wohlbefinden

Szenario	Mögliche Gefährdung
• Allgemeine Nutzung von Apps und/oder Mobilgeräten.	→ Designelemente (z.B. 3D-Effekte, Farben, rasches Wechseln der dargestellten Elemente) lösen Unwohlsein aus.
• Einsatz von Apps mit Augmented oder Virtual Reality Elementen in der medizinischen Aus- und Weiterbildung.	→ Auftreten einer „Cybersickness“ (Kiryu und So 2007, Nalivaiko et al. 2015), deren Symptome in etwa denen der Reisekrankheit entsprechen können.

Seelisches Wohlbefinden

Szenario	Mögliche Gefährdung
• Intensive und über ein normales Maß hinausgehende Nutzung eines Smartphones zu allgemeinen oder gesundheitsbezogenen Zwecken (z.B. Quantified Self, Diät, ...).	→ Bei dafür empfänglichen Patienten potenzieller Auslöser für Depressionen sowie Schlaf und Angststörungen (Demirci, Akgönül und Akpinar 2015), wie es auch bereits für andere digitale Technologien beschrieben wurde (Starevic und Aboujoude 2015).

Persönlichkeitsrechte

Szenario	Mögliche Gefährdung
• Angabe/Eingabe von Symptomen in Patiententagebüchern (Årsand et al. 2013), Symptomcheckern (Semigran et al. 2015), Nachschlagewerken, digitalen Krankenakten, Selbstauskünften zur Tarifierung.	→ Bei unzureichenden Maßnahmen zu Datenschutz und Datensicherheit bzw. Design-Fehlern: Unbeabsichtigte Weitergabe von persönlichen oder die Gesundheit Dritter betreffenden Informationen und Nutzung dieser Informationen zum Nachteil des Nutzers durch Dritte.
• Kommunikation der Krankengeschichte über E-Mail, SMS, durch die Betroffenen selbst oder ihre Behandler (Prochaska et al. 2015).	→ Unbeabsichtigte Preisgabe von persönlichen oder die Gesundheit Dritter betreffenden Informationen durch Übermittlung über ungeschützte Kommunikationskanäle.
• Mitteilung von Erfahrungsberichten über Social Media-Kanäle (Facebook, Twitter, Blogs, Foren, ...), z.B. bei einer seltenen oder stigmatisierenden Erkrankung.	→ Unbeabsichtigte Identifikation Betroffener durch Zusammenführen von im jeweiligen Netzwerk verfügbaren Informationen (Hartz et al. 2013, Hartz et al. 2014) oder Verknüpfung mit Informationen aus sonstigen Datenquellen. → Unbeabsichtigte (und evtl. erst mit zeitlichem Verzug relevante) Bloßstellung von erkrankten Kindern durch Eltern, die z.B. (über Social-Media-Kanäle) Erfahrungsaustausch mit anderen Betroffenen suchen und Jahre später erfolgende Nutzung dieser Informationen zum Nachteil der Betroffenen (z.B. durch Arbeitgeber, Versicherungen, ...).

Fortsetzung auf der nächsten Seite

Fortsetzung Tabelle 3

Szenario	Mögliche Gefährdung
• Informationen über die eigene Genetik bei Stammbaumanalysen; entsprechende Dienste stellen teils webbasierte (evtl. auch durch Apps nutzbare) Schnittstellen bereit bzw. können über Apps angesprochen werden.	→ Unbeabsichtigte Offenlegung von Verwandtschaftsverhältnissen, Erkrankungen etc. mit potenzieller Demaskierung der vermeintlich anonymen „Datenspender" (Hayden 2015) erlauben Rückschlüsse auf die Gesundheit der Betroffenen bzw. ihre gesundheitlichen Risiken.
• Unbeabsichtigte Weitergabe von persönlichen oder die Gesundheit anderer betreffenden Informationen und Nutzung dieser Informationen zum Nachteil des Nutzers durch (unberechtigte) Dritte. Mögliche Auslöser: die Patienten selbst, aber auch ärztliches Personal, das ein (eigenes oder vom Arbeitgeber bereitgestelltes) Smartphone zur fotographischen oder anderweitigen Befunddokumentation einsetzt.	→ Aus scheinbar „harmlosen" Daten lassen sich biometrische und anderweitig identifizierbare Merkmale ableiten, die auch bei vorgeblicher Anonymisierung eindeutige Rückschlüsse auf den Betroffenen zulassen. Beispiele: • Aus aufgezeichneten Audiodaten werden Stimmen identifiziert und zugeordnet; eine Identifizierung ist möglich, genauso, wie eine Einschätzung der aktuellen Gefühlslage, Motivation etc. (Cohen et al. 2015). • Gesichtserkennung aus Bilddaten; gekoppelt mit oft parallel aufgezeichneten und in den Bilddaten gespeicherten Ortsinformationen lassen sich so (Bewegungs-) Profile der Betroffenen herleiten.
• Unzureichend geschützte private Geräte, die im beruflichen Kontext durch medizinisches Personal genutzt wurden, kommen abhanden und es gelangen patientenbezogene Daten in falsche Hände.	→ Nutzung der Daten durch Unbefugte; Mögliche Erpressung der betroffenen Patienten/des medizinischen Personals.

9 Folgerungen

Diverse Maßnahmen sind denkbar, um dem Risikopotenzial wirksam zu begegnen. Um wirksam zu sein, müssen die Aktivitäten den Charakter des dynamischen und liberalen Markts berücksichtigen. Sie müssen ebenso schnell und einfach umzusetzen und individualisierbar sein, um die nötige Flexibilität zu liefern. Hierdurch wird auch die Akzeptanz unter den Akteuren gesteigert werden können.

Entwicklung: Im Rahmen der Planung und Entwicklung von Software sollen Hersteller bereits eine Risikoanalyse durchführen und etwaige Gefahren im Vorfeld identifizieren und beseitigen. Hierzu sollen die gängigen Praktiken in der Softwareentwicklung zum Einsatz kommen. Anleitungen finden sich in entsprechenden Normen, die an entsprechender Stelle ausgeführt werden. Die Entwicklung soll nach üblichen Qualitätskriterien und qualitätsgesichert erfolgen (s. Kapitel 15).

Transparenz: Die Herstellenden sollen über ihr Produkt transparent informieren. Hierzu zählt auch die Mitteilung über Gefahren und Risiken aber auch eingetretene Schäden. Dies kann primär niedrigschwellig in der Produktinformation in den App Stores und auf begleitenden Webseiten erfolgen (s. Kapitel 13).

Vigilanzsystem: Gesundheits-Apps können Gefahren für die Anwenderinnen und Anwender beinhalten. Nachweisliche Schäden sind in der Literatur allerdings nicht beschrieben. Allenfalls werden mögliche Gefahren dargestellt. Zur konkreten Risiko-Nutzen Abschätzung fehlen belastbare Daten. Um diese zu erhalten, wäre die Einrichtung eines niedrigschwelligen Vigilanzsystems ähnlich dem RAPEX-System[5] der EU anzuregen. Dieses soll zentral Meldungen über mögliche und eingetretene Schäden und Nebenwirkungen sammeln und öffentlich bereitstellen. Diese Information soll durch den Hersteller gepflegt werden, da dieser in der Regel im Rahmen der eigenen Produktbeobachtung primär Kenntnis über Vorkommnisse erhält (Kundeninformation, eigene Tests etc.). Ferner sollen die Betreiberinnen und Betreiber (professionelle und Laienanwender) direkt

[5] Rapid Alert System for dangerous non-food products. http://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/index_en.htm [Zugriff 05. März 2016].

Vorkommnisse melden können. Anbieter der Vertriebsplattformen sollen ihre Bemühungen zur Qualitätsverbesserung des Angebots steigern, hierzu sollen sie verbindliche Qualitätsvorgaben etablieren, die sich auch mit der inhaltlichen Qualität der Apps auseinandersetzt. Die internen Reviewverfahren sollen hierzu verbessert werden.

Organisatorische Maßnahmen: Betreiber von Gesundheits-Apps müssen im Einsatzumfeld geeignete Maßnahmen treffen, die Risiken in der Anwendung von Gesundheits-Apps minimieren. Prozesse müssen hierzu eingerichtet werden, sei es in Form von verbindlichen Hygiene-Prozessen in Krankenhäusern, die die Reinigung/Desinfektion von Betreibergeräten vorsehen und Prozesse, die zum Schutz der Patientendaten auf den Betreibergeräten dienen (Sicherheitsrichtlinien für dienstliche Geräte oder dienstlich eingesetzte Privatgeräte (Bring Your Own Device). Ferner sind Fortbildungen und Aufklärungen anzuregen, die die Sensibilität für die Thematik fördern sollen.

Aufklärung: Anwenderinnen und Anwender sind sich möglicher Risiken und Gefahren, die sich aus der Nutzung von Mobilgeräten und Apps ergeben, nur selten bewusst. Zuvorderst muss daher dafür Sorge getragen werden, allen Beteiligten diese auch bewusst zu machen, zum Beispiel im Rahmen von Aufklärungskampagnen, die sich an die breite Öffentlichkeit, aber auch an einzelne Nutzergruppen ebenso wie Anbieter und Entwickler von Apps richten. Je größer das Verständnis der Betroffenen in Bezug auf die Risiken, Gefahren und daraus folgenden (medizinischen, rechtlichen wie ethischen) Konsequenzen, die sich aus der Nutzung der Technologie für sie ergeben können, desto eher werden Maßnahmen, die zur Minimierung der Risiken und Gefahren empfohlen oder auf Organisationsebene bzw. von gesetzlicher Seite angeordnet werden, auch Gehör finden und akzeptiert werden.

Aufklärungsmaßnahmen sollten hierbei – beispielsweise hinsichtlich der Nutzung im professionellen Umfeld – organisatorische Aspekte umfassen, z.B. hinsichtlich der Gestaltung und Anwendung adäquater krankenhausinterner Regelungen, um ein mögliches Organisationsverschulden zu vermeiden (Pramann und Albrecht 2014). Zudem sollte auch über Risiken und Gefahren aufgeklärt werden, die sich sowohl auf medizinischer, aber auch auf Patientenseite aus der Nutzung in diesem sensiblen Kontext ergeben können. Dies umfasst alle in den vorigen Abschnitten genannten Aspekte, von der Vermeidung körperlicher Schäden, negativer Einflussnahme auf das körperliche und seelische Wohlbefinden, aber auch Maßnahmen, die abseits gesundheitlicher Belange dem Datenschutz und der Datensicherheit dienen.

10 Schlüsselergebnisse

- In der Literatur werden unterschiedlichste Gefährdungen beschrieben. Durch Apps bedingte konkrete Schäden finden sich nicht. Analogieschlüsse sind bedingt durch Erfahrungen aus dem Medizinproduktebereich möglich.
- Gesundheitsbezogene Apps haben ein generelles Gefährdungs- und Missbrauchspotenzial, welches sich insbesondere bei fehlerhafter Herstellung oder Anwendung verwirklichen kann.
- Durch Aufklärung und Sensibilisierung aller Akteure für die Problematik, eine qualitätsgesicherte Entwicklung und transparente Produktkommunikation der Hersteller, organisatorische Maßnahmen der Betreiber und die Etablierung eines niedrigschwelligen Vigilanzsystems kann dem Risikopotenzial wirksam begegnet werden.

11 Zusammenfassung

Abgesehen von unmittelbaren Risiken für die Gesundheit bestehen mittelbare Risiken, die sich über negative Auswirkungen auf den sozialen und/oder wirtschaftlichen Status und die persönliche Freiheit auswirken können. Körperliche Schäden und der Missbrauch von persönlichen (Gesundheits-) Daten stehen im Vordergrund. Besonders die Kenntnis möglicher Risiken ist für eine Risiko-Nutzen-Abwägung im Kontext des Einsatzes von Gesundheits-Apps unerlässlich, um die hierunter durchgeführten Maßnahmen individuell und für die Gesellschaft bewerten zu können. Hierzu ist die Datenlage allerdings nicht ausreichend. Zur Reduktion von Risiken sind vielfältige Maßnahmen denkbar. Neben einer umfassenden Aufklärung aller Beteiligten über Gefahren im Kontext mit Gesundheits-Apps und deren Prävention, sollen Herstellerinnen und Hersteller qualitätsgesichert entwickeln, was grundsätzlich eine Risikoanalyse mit einschließt. Ferner ist die Einrichtung eines niedrigschwelligen Vigilanzsystems für Gesundheits-Apps zur schnellen und

breiten Kommunikation sinnvoll. Von Betreiberseite im professionellen Umfeld sind organisatorische Maßnahmen zu treffen, die einen risikoarmen Einsatz ermöglichen. Anwenderinnen und Anwender stehen in der Verantwortung, ihr Handeln unter Zuhilfenahme einer Gesundheits-App intensiver zu prüfen, sensibel gegenüber Risiken zu sein und nach ihrem Vermögen zu einer Qualitätsverbesserung beizutragen, indem sie etwaige Unregelmäßigkeiten, Fehler oder Schäden dem Hersteller, dem Betreiber oder einer anderen geeigneten Stelle melden.

12 Summary

Apart from immediate risks for health, there are also risks that may indirectly endanger an individual's social or financial status as well as personal freedom. Physical harm as well fraudulent use of (health related) data are of primary interest in this context. Knowing what the risks are is also essential for cost-benefits considerations, both on an individual level as well as with respect to society. Unfortunately, the necessary aspects are not adequately covered in literature. Apart from providing comprehensive information for all those concerned about the dangers of health related apps and how to prevent them, manufacturers need to employ quality assurance methods for development and this also includes analyzing the risks. Furthermore, implementing a low-barrier vigilance system for health related apps would provide a means to ensure a fast and broad communication. Also, on the operators' side, especially in a professional context, organizational measures need to be implemented in order to minimize risks arising from the use of apps. And finally, the users themselves are obliged to critically assess their use of health related apps and to be sensitive about potential risks. They should also do everything in their power to help with improving quality by reporting any irregularities, errors or defects they observe to the developers, operators or any other suitable party.

13 Literatur

Årsand, E.; Skrøvseth, S. O.; Hejlesen, O.; Horsch, A.; Godtliebsen, F.; Grøttland, A. & Hartvigsen, G. (2013), Mobile patient applications within diabetes – from few and easy to advanced functionalities, *Stud Health Technol Inform* **192**, 1010.

Albrecht, U.-V.; von Jan, U.; Sedlacek, L.; Groos, S.; Suerbaum, S. & Vonberg, R. P. (2013), Standardized, App-Based Disinfection of iPads in a Clinical and Nonclinical Setting: Comparative Analysis, *J Med Internet Res* **15**(8), e176.

Ali, F. R. (2015), The unadulterated smartphone camera: obviating the need for apps, *J Am Acad Dermatol* **72**(5), e119.

Anthony, S. (2013). iOS 7 nausea and cybersickness: What causes it, and why it's a sign of things to come | ExtremeTech. [online] ExtremeTech. Verfügbar unter http://www.extremetech.com/extreme/167717-ios-7-nausea-and-cybersickness-what-causes-it-and-why-its-a-sign-of-things-to-come [Zugriff 10. Dez. 2015].

Apple (2015). App Store Review Guidelines – Apple Developer. [online] developer.apple.com. Verfügbar unter https://developer.apple.com/app-store/review/guidelines/#damage-device [Zugriff 5. Dez. 2015].

Becker, L. (2013). Apple bewahrt Siri-Daten bis zu zwei Jahre lang auf. [online] Mac & i. Verfügbar unter http://www.heise.de/mac-and-i/meldung/Apple-bewahrt-Siri-Daten-bis-zu-zwei-Jahre-lang-auf-1846278.html [Zugriff 11. Dez. 2015].

BfArM (2011). BfArM – Maßnahmen von Herstellern – Sicherheitshinweis für iPhone-/Android-Applikation „Pfizer Rheumatology Calculator", Pfizer. [online] Bfarm.de. Verfügbar unter http://www.bfarm.de/SharedDocs/Kundeninfos/DE/09/2011/4757-11_Kundeninfo_de.html [Zugriff 5. Dez. 2015].

Ben, S. (2014). Apples Gesundheits-App: Zuckererfassung funktioniert nicht richtig. [online] Mac & i. Verfügbar unter http://www.heise.de/mac-and-i/meldung/Apples-Gesundheits-App-Zuckererfassung-funktioniert-nicht-richtig-2425463.html [Zugriff 19. Dez. 2015].

Bierbrier, R.; Lo, V. & Wu, R. C. (2014), Evaluation of the accuracy of smartphone medical calculation apps, *Journal of medical Internet research* **16**(2):e32.

Borer, A.; Gilad, J.; Smolyakov, R.; Eskira, S.; Peled, N.; Porat, N.; Hyam, E.; Trefler, R.; Riesenberg, K. & Schlaeffer, F. (2005), Cell phones and Acinetobacter transmission, *Emerg Infect Dis* **11**(7), 1160-1161.

CHIP Online, (2015). Diese Bilder machen Angst: iPhone explodiert, Teenager erleidet Verbrennungen. [online] Verfügbar unter http://www.chip.de/news/Diese-Bilder-machen-Angst-iPhone-explodiert-Teenager-erleidet-Verbrennungen_

79179447.html [Zugriff 10. Dez. 2015].

Cohen, A. S.; Renshaw, T. L.; Mitchell, K. R. & Kim, Y. (2015), A psychometric investigation of "macroscopic" speech measures for clinical and psychological science, *Behav Res Methods*.

Demirci, K.; Akgönül, M. & Akpinar, A. (2015), Relationship of smartphone use severity with sleep quality, depression, and anxiety in university students, *J Behav Addict* **4**(2), 85-92.

Deutscher Bundestag (1996), Entwurf eines Gesetzes zur Umsetzung der EG-Rahmenrichtlinie Arbeitsschutz und weiterer Arbeitsschutz-Richtlinien. Drucksache 13/3540. 13. Wahlperiode. Verfügbar unter http://dipbt.bundestag.de/doc/btd/13/035/1303540.pdf [Zugriff 19. Dez. 2015].

DIN EN ISO 14971:2013-04, Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971:2007, korrigierte Fassung 1. Oktober 2007); Deutsche Fassung EN ISO 14971:2012

Endo, Y.; Saito, K.; Kojima, S.; Watanabe, S.; Takahashi, M. & Ito, K. (2013), Evaluation of electromagnetic interference to implanted cardiac pacemaker due to mobile phone, *in* 2013 International Conference on Electromagnetics in Advanced Applications (ICEAA), Institute of Electrical & Electronics Engineers (IEEE), S. 188-191.

ePrivacy GmbH (2015), Datensicherheit und Datenschutz von Medical Apps, Whitepaper.

Fergus, T. A. (2013), Cyberchondria and intolerance of uncertainty: examining when individuals experience health anxiety in response to Internet searches for medical information, *Cyberpsychol Behav Soc Netw* **16**(10), 735-739.

Fernandez-Guerrero, I. M. (2014), WhatsAppitis, *Lancet* **383**(9922), 1040.

Fischer, T (2015), *Strafgesetzbuch mit Nebengesetzen*. 62. Auflage, München: C.H. Beck Verlag.

Flournoy, V. (2010), Medical device recalls. [online] Verfügbar unter http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM219681.pdf [Zugriff 18. Dez. 2015].

Fu, K. (2011), Trustworthy medical device software, *Institute of Medicine Workshop on Public Health Effectiveness of the FDA 510(k) Clearance Process,* Preprint. Verfügbar unter https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf [Zugriff 20. Dez. 2015].

Fu, K. & Blum, J. (2014), Controlling for cybersecurity risks of medical device software, *Biomed Instrum Technol* **Suppl**, 38-41.

Giota, K. G. & Kleftaras, G. (2014), Mental health apps: innovations, risks and ethical considerations, *E-Health Telecommunication Systems and Networks* **3,** 19-23.

Google (2015). Google Play – Vereinbarung für den Entwicklervertrieb. [online] play.google.com. Verfügbar unter https://play.google.com/about/developer-distribution-agreement.html [Zugriff 5. Dez. 2015].

Grimm, J. & Grimm, W. (1854), Deutsches Wörterbuch, von Jacob Grimm und Wilhelm Grimm.

Guze, P. A. (2015), Using Technology to Meet the Challenges of Medical Education, *Trans Am Clin Climatol Assoc* **126**, 260-270.

Hartz, T.; Lablans, M.; Hollinderbäumer, A. & Ückert, F. (2013), Proof-of-Concept–Easily Identifying and Extracting Potential Patients in Facebook, *in* Medicine 2.0 Conference. Verfügbar unter http://www.medicine20congress.com/ocs/index.php/med/med2013/paper/view/1741 [Zugriff 19. Dez. 2015].

Hartz, T.; Storf, H.; Hollinderbäumer, A.; Trautmann, F.; Walter, F. & Ückert, F. (2014), Risk Analysis of Different Use Cases Which Might Lead to Patient Identification within Facebook, *in* Medicine 2.0 Conference. Verfügbar unter http://www.medicine20congress.com/ocs/index.php/med/med2014b/paper/view/2449 [Zugriff 19. Dez. 2015].

Haataja, K. M. & Hypponen, K. (2008), Man-In-The-Middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures, *in* ISCCSP 2008. 3rd International Symposium on Communications, Control and Signal Processing, Institute of Electrical & Electronics Engineers (IEEE), 1096-1102.

Hayden, E. C. (2013), Privacy loophole found in genetic databases, *Nature News*. Verfügbar unter http://www.nature.com/news/privacy-loophole-found-in-genetic-databases-1.12237 [Zugriff 20. Dez. 2015].

Hörmann, H.J. (2015), Human Factor, Handbuch Klinisches Risikomanagement, Springer Science + Business Media, S. 133-146.

Huckvale, K.; Adomaviciute, S.; Prieto, J. T.; Leow, M. K.-S. & Car, J. (2015a), Smartphone apps for calculating insulin dose: a systematic assessment, *BMC Med* **13**, 106.

Huckvale, K.; Morrison, C.; Ouyang, J.; Ghaghda, A. & Car, J. (2015b), The evolution of mobile apps for asthma: an updated systematic assessment of content and tools, *BMC Med* **13**, 58.

Inal, E. E.; Demirci, k.; Çetintürk, A.; Akgönül, M. & Savaş, S. (2015), Effects of smartphone overuse on hand function, pinch strength, and the median nerve, *Muscle Nerve* **52**(2), 183-188.

Israelski, E. & Muto, W. (2011), Human Factors Risk Management for Medical Products' Handbook of Human Factors and Ergonomics in Health Care and Patient Safety, Second Edition, Informa UK Limited, S. 475-506.

Kassianos, A. P.; Emery, J. D.; Murchie, P. & Walter, F. M. (2015), Smartphone applications for melanoma detection by community, patient and generalist clinician users: a

review, *Br J Dermatol* **172**(6), 1507-1518.

Kemnitz, G. (2007), *Test und Verlässlichkeit von Rechnern*, Springer Berlin Heidelberg.

Kiryu, T. & So, R. H. Y. (2007), Sensation of presence and cybersickness in applications of virtual reality for advanced rehabilitation, *J Neuroeng Rehabil* **4**, 34.

Kramer, D. B.; Baker, M.; Ransford, B.; Molina-Markham, A.; Stewart, Q.; Fu, K. & Reynolds, M. R. (2012), Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance, *PLoS One* **7**(7), e40200.

Kuss, D. J. & Griffiths, M. D. (2011), Online social networking and addiction–a review of the psychological literature, *Int J Environ Res Public Health* **8**(9), 3528-3552.

Kuss, D. J. & Griffiths, M. D. (2012), Internet and gaming addiction: a systematic literature review of neuroimaging studies, *Brain Sci* **2**(3), 347-374.

Leveson, N. G. (1995), *Safeware: system safety and computers*, Addison-Wesley Professional.

Leveson, N. G. & Turner, C. S. (1993), An investigation of the Therac-25 accidents, *Computer* **26**(7), 18-41.

Mare, S. & Kotz, D. (2010), Is Bluetooth the right technology for mHealth?, *in* USENIX Workshop on Health Security and Privacy. USENIX Association. Verfügbar unter http://www.cs.dartmouth.edu/~dfk/papers/abstracts/mare-healthsec10.html [Zugriff 19. Dez. 2015].

Mosso, J. L.; Gorini, A.; De La Cerda, G.; Obrador, T.; Almazan, A.; Mosso, D.; Nieto, J. J. & Riva, G. (2009), Virtual reality on mobile phones to reduce anxiety in outpatient surgery, *Stud Health Technol Inform* **142**, 195-200.

Nalivaiko, E.; Davis, S. L.; Blackmore, K. L.; Vakulin, A. & Nesbitt, K. V. (2015), Cybersickness provoked by head-mounted display affects cutaneous vascular tone, heart rate and reaction time, *Physiol Behav* **151**, 583-590.

Papadopoulos, H.; Pappa, D. & Gortzis, L. (2006), Legal & Clinical Risk Assessment Guidelines in Emerging m-Health Systems, *in* Proceeding in ITAB-2006. 6th International IEEE EBMS Special Topic Conference on Information Technology Application in Biomedicine. Ioannina, Greece, S. 24-28.

Papadopoulos, H.; Pappa, D. & Gortzis, L. (2007), A framework for dealing with legal and clinical risks arising from the use of m-health systems, *Journal on Information Technology in Healthcare* **5**(3), 182-195.

Parime, S. & Suri, V. (2014), Cyberbullying detection and prevention: Data mining and psychological perspective, *in* Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference on, S. 1541-1547.

Paul, N.; Kohno, T. & Klonoff, D. C. (2011), A review of the security of insulin pump infusion systems, *J Diabetes Sci Technol* **5**(6), 1557-1562.

Paffi, A.; Apollonio, F.; Pinto, R. & Liberti, M. (2015), Scenarios approach to the electromagnetic exposure: the case study of a train compartment, *Biomed Res Int* **2015**, 869895.

Pfizer (2011), „Pfizer Rheumatology Calculator" iPhone /Android Application – important information. [online] Verfügbar unter http://www.pharma-mkting.com/images/Pfizer_Rheum_BugLetter.pdf [Zugriff 5. Dez. 2015].

Pramann, O. & Albrecht, U.-V. (2014), Smartphones, Tablet-PC und Apps in Krankenhaus und Arztpraxis Smartphones – rechtssicher und erfolgreich einsetzen, Deutsche Krankenhaus Verlagsgesellschaft mbH.

Poulsen, A. H.; Friis, S.; Johansen, C.; Jensen, A.; Frei, P.; Kjaear, S. K.; Dalton, S. O. & Schüz, J. (2013), Mobile phone use and the risk of skin cancer: a nationwide cohort study in Denmark, *Am J Epidemiol* **178**(2), 190-197.

Pournaghshband, V.; Meyer, D.; Holyland, M.; Sarrafzadeh, M. & Reiher, P. (2014), Adrasteia: A Smartphone App for Securing Legacy Mobile Medical Devices, *in* 17th International Conference on Computational Science and Engineering (CSE), 2014 IEEE, S. 758-763.

Prochaska, M. T.; Bird, A.-N.; Chadaga, A. & Arora, V. M. (2015), Resident Use of Text Messaging for Patient Care: Ease of Use or Breach of Privacy?, *JMIR Med Inform* **3**(4), e37.

Radcliffe, J. (2011), Hacking medical devices for fun and insulin: Breaking the human SCADA system, *in* Black Hat Conference presentation slides.

Repacholi, M. H.; Lerchl, A.; Röösli, M.; Sienkiewicz, Z.; Auvinen, A.; Breckenkamp, J.; d'Inzeo, G.; Elliott, P.; Frei, P.; Heinrich, S.; Lagroye, I.; Lahkola, A.; McCormick, D. L.; Thomas, S. & Vecchia, P. (2012), Systematic review of wireless phone use and brain cancer and other head tumors, *Bioelectromagnetics* **33**(3), 187-206.

Rossignol, J. (2015). Apple Removes Over 250 iOS Apps With Ad SDK That Collects Personal User Data. [online] Macrumors.com. Verfügbar unter http://www.macrumors.com/2015/10/19/apple-to-remove-hundreds-apps-youmi-sdk/ [Zugriff 5. Dez. 2015].

Semigran, H. L.; Linder, J. A.; Gidengil, C. & Mehrotra, A. (2015), Evaluation of symptom checkers for self diagnosis and triage: audit study, 351:h3480.

Sharan, D.; Mohandoss, M.; Ranganathan, R. & Jose, J. (2014), Musculoskeletal disorders of the upper extremities due to extensive usage of hand held devices, *Ann Occup Environ Med* **26**, 22.

Spiegel Online (2010). Peinliche Panne: McAfee-Update schießt Windows XP ab – SPIEGEL ONLINE. [online] SPIEGEL ONLINE. Verfügbar unter http://www.spiegel.de/netzwelt/

gadgets/peinliche-panne-mcafee-update-schiesst-windows-xp-ab-a-690505.html [Zugriff 18. Dez. 2015].

Starcevic, V. & Aboujaoude, E. (2015), Cyberchondria, cyberbullying, cybersuicide, cybersex: "new" psychopathologies for the 21st century?, *World Psychiatry* **14**(1), 97-100.

Steele, D. (2015). Fraudulent Application Removed From Google Play Store. [online] AndroidHeadlines.com. Verfügbar unter: http://www.androidheadlines.com/2015/07/fraudulent-application-removed-google-play-store.html [Zugriff 5. Dez. 2015].

Sunyaev, A.; Dehling, T.; Taylor, P. L. & Mandl, K. D. (2015), Availability and quality of mobile health app privacy policies, *J Am Med Inform Assoc* **22**(e1), e28-e33.

syracuse.com (2010). University Hospital computers plagued by anti-virus glitch. [online] Verfügbar unter http://www.syracuse.com/news/index.ssf/2010/04/university_hospital_plagued_by.html [Zugriff 18 Dez. 2015].

Tillmann, H. (2012), Browser Fingerprinting: Tracking ohne Spuren zu Hinterlassen, Diplomarbeit, Humboldt-Universität zu Berlin.

Walia, S. S.; Manchanda, A.; Narang, R. S.; N, A.; Singh, B. & Kahlon, S. S. (2014), Cellular telephone as reservoir of bacterial contamination: myth or fact, *J Clin Diagn Res* **8**(1), 50-53.

Weber, M. (2015), Leitlinien für den Big-Data-Einsatz. Chancen und Verantwortung, Technical report, Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Wetter, T. (2015), Consumer Health Informatics: New Services, Roles, and Responsibilities, Springer.

Wicks, P. & Chiauzzi, E. (2015), "Trust but verify" – five approaches to ensure safe medical apps, *BMC Med* **13**, 205.

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 dermatology* **149**(4), 422-426.