Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer

Überblick der wichtigsten Grundbegriffe und Prozesse bei der Abgrenzung, Entwicklung und Inverkehrbringung einer App als Medizinprodukt

Bern, 02. März 2018

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

Centre de compétences et de coordination
de la Confédération et des cantons

Centro di competenza e di coordinamento
di Confederazione e Cantoni

Impressum

© eHealth Suisse, Kompetenz- und Koordinationsstelle von Bund und Kantonen

Autoren: Hansjörg Riedwyl, ISS AG, Integrated Scientific Services, Biel

Lizenz: Dieses Ergebnis gehört eHealth Suisse (Kompetenz- und Koordinationsstelle von Bund und Kantonen). Das Schlussergebnis wird unter der Creative Commons Lizenz vom Typ „Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 Lizenz“ über geeignete Informationskanäle veröffentlicht. Lizenztext: http://creativecommons.org/licenses/by-sa/4.0

Identifikation dieses Dokuments
OID: 2.16.756.5.30.1.127.1.3.5.1.1

Weitere Informationen und Bezugsquelle:
www.e-health-suisse.ch

The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Zweck und Positionierung dieses Dokuments

Ziel ist die Förderung des Grundverständnisses für regulatorische Themen von mHealth Apps, die Vermittlung eines Überblicks der wichtigsten Grundbegriffe und Prozesse bei der Abgrenzung, Entwicklung und Inverkehrbringung einer App als Medizinprodukt.

Im Interesse einer besseren Lesbarkeit wird auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangslage

Einleitung

Mit der Markteinführung des Smartphones hat sich in der Software-Entwicklung ein neues Entwicklungsfeld geöffnet. Apps zu diversen Themen sind gefragt und werden rege von Anwendern genutzt. Gerade Anwendungen zu medizinischen oder Lifestyle-Themen erscheinen zahlreich und mit einem sehr breiten Fokus. Sind medizinische Fragestellungen und Anwendungen involviert, muss sich ein Entwickler frühzeitig die Frage stellen, ob seine App nicht auch ein Medizinprodukt – und somit zertifizierungspflichtig – sein könnte. Diese Fragestellung wird aktuell häufig zu spät im Design-Prozess gestellt. Deshalb – und auch im Hinblick auf die europäische Neuregulierung von Medizinprodukten und In-vitro-Diagnostika – wurde dieser Leitfaden als Hilfestellung zur Unterscheidung von Lifestyle- / Wellnessprodukten und Medizinprodukten und für die Vorbereitung und Durchführung des Zertifizierungsprozesses erarbeitet. Zusätzlich zu diesen Themen soll der Leitfaden auch auf Themen aufmerksam machen, die über die Zertifizierung (MepV) hinausgehen. Dazu gehören zum Beispiel Risiken, die mit dem Einsatz von mHealth-Lösungen verbunden sind und bereits bei der Entwicklung Beachtung finden müssen. Dies sind unter anderem die Themen Datenschutz und -sicherheit. Der Leitfaden soll Entwickler, Inverkehrbringer, Soft- und Hardware-Hersteller für Themen sensibilisieren, die für die Anwender von Bedeutung sind. Er zielt auch darauf ab, dass mehr Transparenz für die Endnutzer im Bereich der mHealth-Lösungen geschaffen wird.

1.2 Inhalt und Haftung

1.2.1 Leitfaden und Checklisten

Der Leitfaden soll praktische Hilfestellung geben, ob eine App als Medizinprodukt zu qualifizieren ist und welche regulatorischen Vorschriften zu erfüllen sind. Zudem soll der Leitfaden aufzeigen, wo Risiken in der Entwicklung liegen und wie ein optimaler Entwicklungsprozess ablaufen kann.

Der Leitfaden besteht aus einem ausführlichen Grundlagenkapitel sowie drei themenspezifischen Kapiteln. Den Abschluss bilden ein Glossar und eine Linkliste. Jeweils auf der rechten Seite befindet sich eine Kommentarspalte mit nützlichen Links sowie einigen zusammenfassenden Stichworten zur Textpassage.

Jedes Kapitel enthält zudem zu Beginn eine Kurzzusammenfassung der wesentlichen Inhalte.
Ergänzend zum Leitfaden gibt es acht Checklisten, die unabhängig vom Leitfaden genutzt werden können. Die Checklisten dienen der Qualitäts- und Prozesssicherung und sollen den Entwickler durch zentrale Fragestellungen anleiten ein sicheres und konformes Medizinprodukt zu entwickeln.

1.2.2 Disclaimer

Die Ersteller übernehmen keinerlei Gewähr hinsichtlich der inhaltlichen Richtigkeit, Genauigkeit, Aktualität, Zuverlässigkeit und Vollständigkeit der bereitgestellten Informationen. Haftungsansprüche gegen die Autoren durch Schäden materieller oder immaterieller Art, welche aus der Nutzung bzw. Nichtnutzung des Leitfadens entstanden sind, werden ausgeschlossen. Die Haftung für Verweise und Links auf Webseiten Dritter liegen ausserhalb des Verantwortungsbereiches des Erstellers dieses Leitfadens. Es wird jegliche Verantwortung für solche Webseiten abgelehnt. Der Zugriff und die Nutzung solcher Webseiten erfolgen auf eigene Gefahr des Anwenders.

1.2.3 Scope

Der Leitfaden fokussiert auf die regulatorische und gesetzliche Situation in der Schweiz. Zudem wird die innereuropäische Sicht betrachtet, wo dies notwendig und sinnvoll erscheint. Weitere Länder, wie zum Beispiel die USA, werden nicht behandelt.
Produktspezifisch fokussiert der Leitfaden auf mobile Software-Medizinprodukte wie Apps.

2 Grundlagen

2.1 Das Wichtigste in Kürze

Die Definition von Medizinprodukten ist gesetzlich in der schweizerischen Medizinprodukteverordnung definiert und entspricht als Umsetzung der europäischen Medizinrichtlinie dem gesamteuropäischen Rechtsrahmen zu Medizinprodukten. Gemäss der Definition kann auch Software als Medizinprodukt qualifiziert werden und somit den gesetzlichen Anforderungen an Sicherheit und Leistung unterliegen. Ausschlaggebend ist dabei die vom Hersteller definierte Zweckbestimmung der Software. Aufgrund der Revision der europäischen Medizinprodukterichtlinie werden Medizinprodukte in Zukunft strenger reguliert und medizinische Software in vielen Fällen einer höheren Risikoklasse zugeordnet. Zusätzlich zur Definition gibt es weitere Dokumente, die zur Entscheidungshilfe bei der Zuordnung zu Medizinprodukten bei Software dienen können (allen voran MEDDEV 2.1/6). Medizinprodukte müssen mit den gesetzlichen Vorgaben konform sein und für den Nachweis der Konformität einen Zertifizierungsprozess durchlaufen. Dieser Prozess sieht abhängig von der zugehörigen Risikoklasse anders aus, denn je höher die Risikoklasse, desto höher sind die Anforderungen an das Produkt. Um nachzuweisen, dass ein Produkt den Anforderungen entspricht, kann auf Normen zurückgegriffen werden, bei harmonisierten Normen ist dies sogar vorgesehen. Ist eine Software gemäss gesetzlicher Definition kein Medizinprodukt, empfiehlt es sich trotzdem den Qualitätsanforderungen gerecht zu werden und involvierte Normen bei der Entwicklung zu beachten. Die Anforderungen betreffend Datenschutz und -sicherheit betreffen alle Apps und sind unabhängig der Zuordnung zu Medizinprodukten verpflichtend.

2.2 Was ist ein Medizinprodukt?

Definition

Die schweizerische Medizinprodukteverordnung definiert in Artikel 1 Medizinprodukte wie folgt:)

Medizinprodukte sind einzeln oder miteinander verbunden verwendete Instrumente, Apparate, Vorrichtungen, Software, Stoffe, Zubehör oder andere medizinisch-technische Gegenstände, einschliesslich der speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinprodukts eingesetzten Software:

a. die zur Anwendung beim Menschen bestimmt sind;

b. deren bestimmungsgemässe Hauptwirkung im oder am menschlichen Körper nicht durch pharmakologische, immunologische oder metabolische Mittel erreicht wird, deren Wirkungsweise durch solche Mittel aber unterstützt werden kann; und

c. die dazu dienen:

1. Krankheiten zu erkennen, zu verhüten, zu überwachen, zu behandeln oder zu lindern,

2. Verletzungen oder Behinderungen zu erkennen, zu überwachen, zu behandeln oder zu lindern oder Behinderungen zu kompensieren,
3. den anatomischen Aufbau zu untersuchen oder zu verändern, Teile des anatomischen Aufbaus zu ersetzen oder einen physiologischen Vorgang zu untersuchen, zu verändern oder zu ersetzen,
4. die Empfängnis zu regeln oder Diagnosen im Zusammenhang mit der Empfängnis zu stellen

Klassische Medizinprodukte, AIMD, IVD

Sie werden unterteilt in:

- klassische Medizinprodukte → z.B. Pflaster, Zahnimplantat, Blutdruckmessgerät, allenfalls auch eine App
- Medizinprodukte für die In-vitro-Diagnostik→ z.B. Schwangerschaftstest, Urintests
- aktive implantierbare Medizinprodukte→ z.B. Herzschrittmacher

Swissmedic

Die zentrale schweizerische Überwachungsbehörde für Heilmittel (Medizinprodukte, Arzneimittel, klinische Studien) ist Swissmedic. Die Swissmedic hat ihren Hauptsitz in Bern und fungiert als öffentlich-rechtliche Anstalt des Bundes mit einer eigenständigen Organisation und Betriebsführung sowie einem eigenen Budget.
Politisch ist die Swissmedic dem EDI (Eidgenössisches Departement des Innern) angegliedert. Dieses schliesst jährlich eine Leistungsvereinbarung mit Swissmedic ab, die den Leistungsauftrag konkretisiert. Der Leistungsauftrag selber wird vom Bundesrat definiert und basiert auf dem Heilmittelrecht.
Wichtig: Swissmedic ist für die Überwachung, aber nicht für die Zertifizierung von Medizinprodukten zuständig.

Infovideos Swissmedic

Die Swissmedic bietet auf ihrer Homepage kurze, informative Videos zu folgenden Themen an:

- „Was ist ein Medizinprodukt“
- „Wie kommt ein Medizinprodukt auf den Markt“
- „Was sind die Aufgaben von Swissmedic im Bereich der Medizinprodukte? “

2.3 Gesetzliche Grundlagen in der Schweiz

Der freie Warenverkehr in Europa (New Global Approach) ermöglicht einen einfachen und schnellen Marktzugang, aber auch eine hohe Eigenverantwortung der Firmen. Diese sind für die Konformität sowie

Erfüllung der grundlegenden Anforderungen selber verantwortlich und müssen diese jederzeit nachweisen können.

Bilaterale Verträge

Die Schweiz hat mit EU-Mitgliedstaaten, EFTA-Staaten und der Türkei Staatsverträge über die gegenseitige Anerkennung von Konformitätsbewertungen für Medizinprodukte abgeschlossen (Bilaterale Abkommen bzw. Mutual Recognition Agreements MRA). Basis für diese Verträge sind die Umsetzung der europäischen Medizinprodukterichtlinien und die europäische CE-Markierung. Die Vertragsstaaten anerkennen die Zertifikate der schweizerischen Konformitätsbewertungsstellen. Umgekehrt anerkennt die Schweiz Konformitätsbewertungen, die durch Benannte Stellen (Notified Bodies) bzw. Konformitätsbewertungsstellen (Conformity assessment bodies) der Vertragsstaaten durchgeführt wurden.

Diese Verträge vereinfachen Meldepflichten der Inverkehrbringer und erlauben einen Direktvertrieb von der Schweiz aus in alle EU- und EFTA-Mitgliedstaaten sowie in die Türkei, dies ohne einen Bevollmächtigten mit Sitz in diesen Ländern. Umgekehrt können Firmen mit Sitz in den Vertragsstaaten konforme Medizinprodukte direkt in der Schweiz vertreiben. Unabhängig davon gelten in den einzelnen Vertragsstaaten weiterhin die landesspezifischen Anforderungen, welche Medizinprodukte betreffen (z.B. Meldepflichten für neue Produkte, Anforderungen betreffend notwendige Sprachen für Produktinformationen, Vorschriften über Rezeptpflicht, berufliche Anwendung der Produkte, Anforderungen an Distributionskanäle, Abgabestellen an das Publikum, Werbung, Rückerstattung durch Sozialversicherungen).

Die wichtigsten Rechtsgrundlagen in der Schweiz sind:

- Bundesgesetz über Arzneimittel und Medizinprodukte — Heilmittelgesetz HMG
- die Medizinprodukteverordnung — MepV
- das Bundesgesetz über die Forschung am Menschen — Humanforschungsgesetz HFG
- die Verordnung über klinische Versuche in der Humanforschung — Verordnung über klinische Versuche KlinV

Diese Rechtstexte setzen Anforderungen der europäischen Medizinprodukterichtlinien in schweizerisches Recht um und beschreiben zusätzliche nationale Vorschriften. Für den Vollzug des Heilmittelgesetzes sorgen die Swissmedic und die kantonalen Behörden.

Hier finden Sie weitere Informationen des EDA zu den Bilateralen Verträgen.

2.4 Gesetzliche Grundlagen in Europa

Auf europäischer Ebene sind Medizinprodukte aktuell durch drei verschiedene Richtlinien geregelt:

- Richtlinie über Medizinprodukte
- Richtlinie über In-vitro-Diagnostika
- Richtlinie über aktive implantierbare medizinische Geräte

Aktuelle Richtlinien
93/42/EWG (MDD)
98/79/EG (IVDD)
90/385/EWG (AIMD)
Künftige Regularien
2017/745 (MDR)
2017/746 (IVDR)

Im Mai 2017 traten die neuen Verordnungen über Medizinprodukte (MDR) und In-vitro-Diagnostika (IVDR) in Kraft. Die MDR wird die bestehenden Richtlinien MDD und AIMD, die IVDR die IVDD ersetzen. Es wurde eine Umsetzungsfrist von 3 (MDR) bzw. 5 Jahren (IVDR) vereinbart. Die AIMD wird aufgehoben und in die MDR integriert.
Die Revision der bestehenden europäischen Medizinprodukte-, IVD- und AIMD-Richtlinien bedeutet für die Hersteller, Distributoren und Lieferanten etc. grosse Umstellungen und Herausforderungen. Alle Produkte müssen unter der MDR neu zertifiziert werden (kein grandfathering), es gibt neue Klassifizierungsregeln (z.B. zu Software oder Nanotechnologie) und die Anforderungen an klinische Daten sowie Post Market Surveillance etc. steigen beträchtlich.
Zu den wichtigsten Änderungen gehören:

- Die technische Dokumentation muss wesentlich detaillierter erstellt werden und verfügbar sein
- Alle Medizinprodukte müssen den UDI=Unique Device Identifier aufweisen.
- Jede Firma muss eine „qualified person“ bestimmen, die über qualifiziertes Fachwissen auf dem Gebiet der Medizinprodukte verfügt.
- Die klinischen Bewertungen werden detaillierter verlangt, wobei auch PMS Daten bei einer Aktualisierung miteinbezogen werden müssen.
- Es gibt neue Klassifizierungsregeln (z.B. Nanotechnologie)
- Die Klassifizierung einiger Produkte ändert sich ebenfalls (z.B. werden viele Software-Produkte von Klasse I zu Klasse IIa hochgestuft).

2.5 Wann ist eine Software ein Medizinprodukt?

Definition

Software kann für verschiedene medizinische Zwecke benutzt werden. Man unterscheidet dabei zwischen *Standalone Software* (eigenständige Software, die aufgrund der Zweckbestimmung als Medizinprodukt qualifiziert wird), Software, welche Teil eines Medizinprodukts ist und Software, die zum Zubehör gehört. Wird eine eigenständige Software als Medizinprodukt qualifiziert, gehört es in die Gruppe der aktiven Medizinprodukte.

Apps und Standalone Software

Da die Zweckbestimmung entscheidend ist für die Qualifizierung als Medizinprodukt, ist auch nachvollziehbar, warum Software und medizinische Apps als Medizinprodukte gelten und deren Anforderungen entsprechen müssen.

Merkblatt Swissmedic

So sind zum Beispiel folgende Apps als Medizinprodukte zu qualifizieren:

- Apps zur Diagnosestellung (z.B. Analyse des Herzrhythmus)
- Apps, die ein Medizinprodukt bedienen (z.B. die Lautstärke eines Hörgerätes verändern)
- Apps, die zur spezifischen und individuellen Auswertung von Patientendaten genutzt werden und Therapievorschläge bieten (z.B. Verhütungskalender mit individueller Anzeige)
- Apps, die die Medikamentendosis berechnen (z.B. Vorschläge für Korrekturinsulin)

Es ist nicht immer einfach zu entscheiden, ob eine Standalone Software als Medizinprodukt einzuordnen ist. Das Merkblatt der Swissmedic hilft bei der Entscheidung und klärt die wichtigsten Begriffe und Punkte.

MEDDEV

Die ausführlichste Entscheidungshilfe, ob es sich bei einer Standalone Software um ein Medizinprodukt handelt, bietet die MEDDEV 2.1/6.

Arbeitsgruppen im näheren Umfeld der EU-Kommissionen erarbeiten MEDDEV-Dokumente (**MED**ical **DEV**ices) als Hilfestellungen. Die MEDDEV-Dokumente sind rechtlich nicht bindend, geben aber Leitlinien und Hilfestellung bei der Interpretation der MDD, AIMD und IVDD.

Für Standalone Software bietet die MEDDEV 2.1/6 Kriterien und Beispiele für die Einstufung von eigenständiger Software als mögliches Medizinprodukt nach der MDD und IVDD.

Ein darin enthaltener Flowchart hilft bei der Entscheidungsfindung:

Flowchart MEDDEV 2.1/6

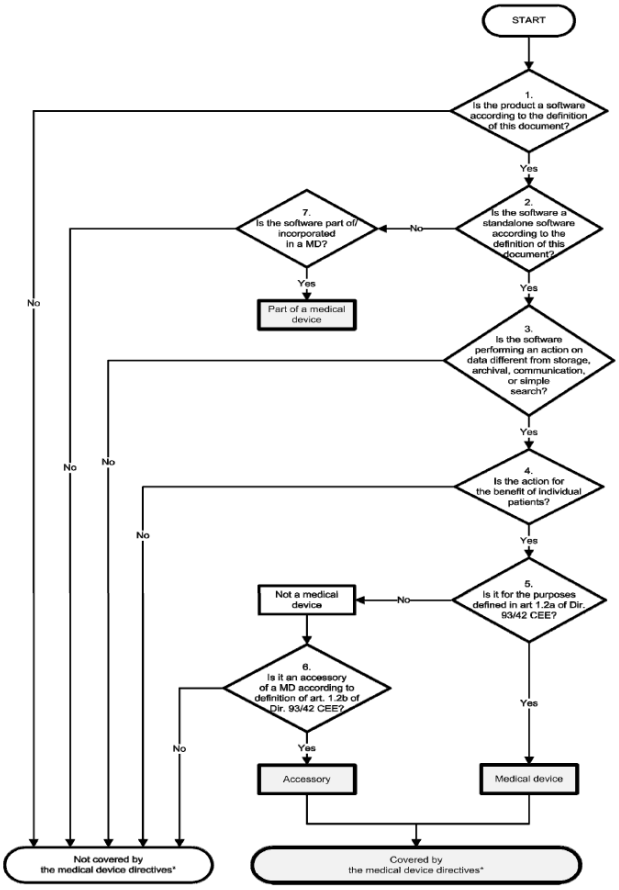

Abbildung 1 Entscheidungsdiagramm ob Software ein Medizinprodukt ist oder nicht

Produkte, bei denen nicht eindeutig klar ist, ob sie unter die Medizinproduktegesetzgebung fallen, werden Borderline-Produkte genannt. Die „Medical Device Expert Group on Borderline and Classification“ der Europäischen Kommission veröffentlicht dazu Entscheidungen betreffend Borderline-Produkten, die für die Auslegung interessant sind. Die neuste Fassung des Manuals enthält zwei neue Entscheidungen zu medizinischen Apps.

Manual on Borderline and Classification in the Community regulatory framework for medical Devices

2.6 Meine Software ist kein Medizinprodukt. Was nun?

Kein Medizinprodukt

Wenn eine Software die MDD-Definition eines Medizinprodukts nicht erfüllt und aufgrund des MEDDEV-Flowcharts nicht als Medizinprodukt eingestuft werden kann, dann ist eine Zertifizierung als Medizinprodukt nicht möglich.

Die in diesem Leitfaden definierten Entwicklungsprozesse und Normen spielen bei der Entwicklung einer Lifestyle/Health/Wearables-App dennoch eine zentrale Rolle. Wird ein Produkt nach diesen Grundsätzen entwickelt und werden die wichtigen Normen wie Usability oder Software-Life-Cycle berücksichtigt, so kann der Entwickler

sichergehen, dass sein Produkt alle notwendigen Stufen durchlaufen hat, um als sicher und zuverlässig zu gelten. Gerade die Entwicklung entlang zentraler, anerkannter Normen kann bei der Vermarktung des Produkts eine wichtige Rolle spielen.
Die Benutzung der Checklisten stellt zudem eine Qualitätssicherungsmassnahme dar und dokumentiert die zentralen Schritte im Entwicklungsprozess.

2.7 Risikoklassen von Medizinprodukten

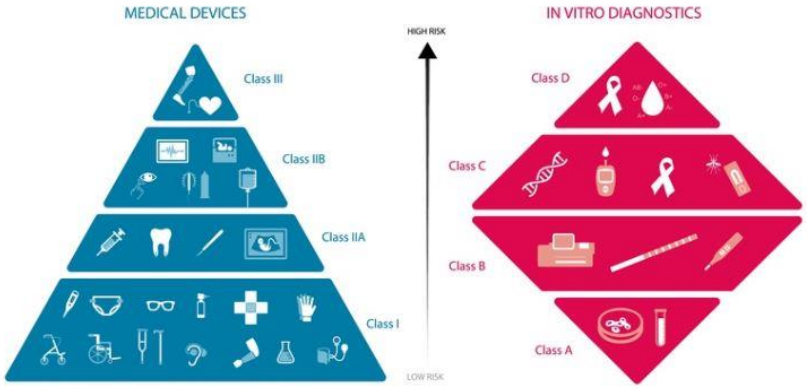

Abbildung 2 Risikoklassen MD und IVD EU (Quelle: MedTech Europe)

Risikoklassen MD

In Europa werden Medizinprodukte in vier Risikoklassen eingeteilt: Bei klassischen Medizinprodukten erfolgt die Einteilung in die Klassen I, IIa, IIb und III nach Anhang IX der Richtlinie 93/42/EWG, wobei die Produktinformation immer zu berücksichtigen ist. Abhängig von Verwendungszweck, Anwendungsdauer und der anatomischen Lage des Produkts können ähnliche Produkte zu unterschiedlichen Klassen gehören.

Risiko-klasse	*Klasse I (geringes Risiko)*	*Klasse IIa (geringes bis mittleres Risiko)*	*Klasse IIb (mittleres bis hohes Risiko)*	*Klasse III (hohes Risiko)*
Beispiele	*Heftpflaster, Korrektionsbrillen*	*Kontaktlinsen, Zahnfüllstoffe, Trachealtuben*	*Röntgengeräte, Harnröhrenstents*	*Kardiovaskuläre Katheter, Hüft-, Schulter- und Kniegelenksprothesen, Herzschrittmacher*

Abbildung 3 Richtlinie 93/42/EWG über Medizinprodukte Artikel 9

Risikoklassen IVD

Für die Klassifizierung von IVDs sind zwei Aspekte abzuklären: einerseits die Zugehörigkeit zur Liste A oder B in Anhang II der Richtlinie 98/79/EG, andererseits eine vorgesehene Eigenanwendung. Mit der neuen IVDR gibt es neu nun 4 Klassen statt 2 Listen:

Risikoklasse	*Anhang II Liste A (hoch kritische IVD's)*	*Anhang II Liste B (kritische IVD's)*	*Produkte zur Eigenanwendung*	*Sonstige*
*Neu nach IVDR**	*D*	*C*	*B*	*A*
Beispiele	*Blutgruppen, HIV, Hepatitis*	*Infektionskrankheiten, Zytomegalovirus, Chlamydien*	*Schwangerschaftstest*	*Laborgerät*

Abbildung 4 Richtlinie 98/79/EG über In-Vitro-Diagnostika Artikel 9

* die Klassifizierung unter der IVDD war auch in A-D eingeteilt. In der IVDR gibt es nach wie vor die Klassen A-D, das Klassifizierungskonzept hat sich allerdings grundlegend verändert.

2.8 Zertifizierung von Medizinprodukten

Notified Bodies und Konformitätsbewertung

Um ein Medizinprodukt auf den Markt zu bringen, muss es allen anwendbaren EU-Richtlinien entsprechen und ein rechtmässiges Konformitätsbewertungsverfahren erfolgreich durchlaufen haben. Die Konformität wird dann durch ein CE-Zeichen auf dem Medizinprodukt sichtbar gemacht.
Im europäischen Raum wird diese Konformität durch sogenannte Benannte Stellen (Notified Bodies) geprüft. Benannte Stellen sind unabhängige, staatlich autorisierte Drittfirmen, die im Auftrag der Medizinproduktehersteller die Konformitätsbewertung vornehmen. Die Wahl der Benannten Stelle steht dem Hersteller frei, solange die Benannte Stelle von der zuständigen Behörde im betreffenden EWR-Staat, in der Schweiz oder der Türkei akkreditiert ist und die jeweilige Produktgruppe in ihrem Scope hat.

NANDO
NBOG

Informationen zu den Benannten Stellen finden sich im Informationssystem NANDO (New Approach Notified and Designated Organisations). Ein Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft regelt die gegenseitige Anerkennung von Konformitätsbewertungen. Entsprechende Vorgaben und Verfahren dazu sind in diversen Richtlinien und Leitfäden der EU-Arbeitsgruppe NBOG (Notified Bodies Operation Group) festgelegt.

CE Eigenverantwortung

Unter Eigenverantwortung des Herstellers werden folgende Medizinprodukte mit einem CE-Zeichen ohne Identifikationsnummer gekennzeichnet:

- Sonderanfertigungen (spezifisch hergestellt für einen Patienten)
- Systeme und Behandlungseinheiten (zusammengestellt aus konformen Medizinprodukten und Zubehör nach Anweisung des Herstellers)
- klassische Medizinprodukte der Klasse I (unsteril und ohne Messfunktion)
- Medizinprodukte für die In-vitro-Diagnostik (ausser solche gemäss Anhang II der Richtlinie 98/79/EG und Produkte zur Eigenanwendung)

Der Hersteller ist dabei selbst verantwortlich, dass seine Produkte die grundlegenden Anforderungen sowie die notwendigen EU-Richtlinien erfüllen.

Die MDD versteht unter grundlegenden Anforderungen alle Minimalanforderungen, die ein Medizinprodukt erfüllen muss, das unter die Richtlinie fällt. Diese grundlegenden Anforderungen werden in Anhang 1 der MDD beschrieben. Als grundlegende Anforderungen gelten beispielsweise die Anforderungen nach

- einem Risikomanagement, das ein positives Nutzen-Risikoverhältnis gewährleistet
- dem Nachweis elektrischer oder mechanischer Sicherheit
- der Gebrauchstauglichkeit
- …

CE mit Benannter Stelle

Eine Bewertung und periodische Überprüfung durch eine Benannte Stelle (Notified Body) ist für folgende Produkte vorgeschrieben:

- sterile Medizinprodukte der Klasse I (Is)
- Medizinprodukte der Klasse I mit Messfunktion (Im)
- Medizinprodukte der Klassen IIa, IIb und III
- aktive implantierbare Medizinprodukte
- In-vitro-Diagnostika nach Anhang II der Richtlinie 98/79/EG
- In-vitro-Diagnostika zur Eigenanwendung

Abhängig von der Klassifizierung und Zweckbestimmung des Produkts (siehe Kapitel 2.5.) hat der Hersteller die Wahl zwischen verschiedenen Zertifizierungswegen, den sogenannten Konformitätsbewertungsverfahren.

Das zur Anwendung kommende Verfahren richtet sich nach der Risikoklasse des Produktes.
Bei Unsicherheiten ist es zu empfehlen, das ausgewählte Verfahren mit der Benannten Stelle zu besprechen. Sobald das Konformitätsbewertungsverfahren erfolgreich abgeschlossen wurde, darf der Hersteller seine Produkte mit dem CE-Kennzeichen versehen. Abhängig von der Risikoklasse muss zudem die Kennnummer der zuständigen Benannten Stelle angebracht werden. Zudem erhält der Hersteller das entsprechende CE-Zertifikat. Der Hersteller kann seine Produkte nun konform in Verkehr bringen.

Konformitätsbewertungsverfahren MDD

Wie bereits erwähnt, unterscheiden sich die Konformitätsbewertungsverfahren nach Risikoklasse. Eine Übersicht der verschiedenen Verfahrenswege hat das britische MHRA hier veröffentlicht.

Konformitätsbewertungsverfahren MDR

Unter der MDR (neue Regulierung) ändern sich die einzelnen Konformitätsbewertungsverfahren. Der TüV Süd hat die neuen Wege grafisch zusammengefasst.

2.9 Involvierte Normen

Definition Norm

Unter einer Norm versteht man ein Dokument, das charakteristische Eigenschaften und Merkmale eines Produkts, eines Prozesses oder einer Dienstleistung beschreibt. Der Schweizerische Normenverband SNV weist in seiner Definition des Begriffes Norm selber auf eine Norm hin:
„Gemäss Definition aus der Norm SN EN ist eine Norm ein Dokument, das ... für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für die Tätigkeiten oder deren Ergebnisse festlegt ...“

Normen werden durch nationale oder internationale Normenkommissionen (IEC, ISO, …) geschrieben und sind ein Basiskonsens aller Beteiligten.
Grundsätzlich ist eine Norm eine Empfehlung und ihre Anwendung freiwillig.

Normung (SECO)

Einige Normen, die sogenannten harmonisierten Normen, werden von europäischen Normungsorganisationen (ISO, CEN, CENELEC, ETSI) aufgrund eines von der EU-Kommission erteilten Mandates erarbeitet. Die Harmonisierungsrechtsvorschriften der EU legen für das Inverkehrbringen eines Produkts die wesentlichen Anforderungen an das Produkt fest. Wird nun ein Produkt nach

harmonisierten Normen hergestellt, so geht man automatisch von einer Erfüllung dieser wesentlichen Anforderungen aus (Konformitätsvermutung).

Da es nicht immer möglich ist, alle Anforderungen an ein Medizinprodukt durch harmonisierte Normen abzudecken, können auch nationale Normen herangezogen werden.
Wenn aber eine harmonisierte Norm existiert und diese nicht angewendet wird, muss der Hersteller Nachweisen, dass sein Produkt den in den grundlegenden Anforderungen definierten Voraussetzungen entspricht.
Für Medizinprodukte sind zahlreiche Normen (national sowie auch harmonisiert) verfügbar. Besonderes Augenmerk in der Entwicklung liegt auf dem Risikomanagement (ISO 14971) sowie der Usability (IEC 62366).
Durch ein entsprechendes Risikomanagement soll der Hersteller frühzeitig das Gefährdungspotenzial seines Produkts erkennen, einschätzen und mindern. Die Risiken werden bewertet und kontrolliert und die Wirksamkeit der Kontrollen nach festgelegten Abläufen überprüft. Dieses Vorgehen erhöht die Sicherheit der Produkte.
Die Usability (Gebrauchstauglichkeit) dient einerseits dazu, dass Produkt anwenderfreundlicher zu machen z.B. durch Berücksichtigung der technischen Kenntnisse oder des Fachwissens, andererseits die Umgebungsfaktoren und ergonomischen Eigenschaften so zu gestalten, dass das Fehlerrisiko gemindert und die Anwendung nutzerfreundlicher wird.
Nachstehende Grafik zeigt den Zusammenhang zwischen den Normen und den gesetzlichen Vorgaben auf:

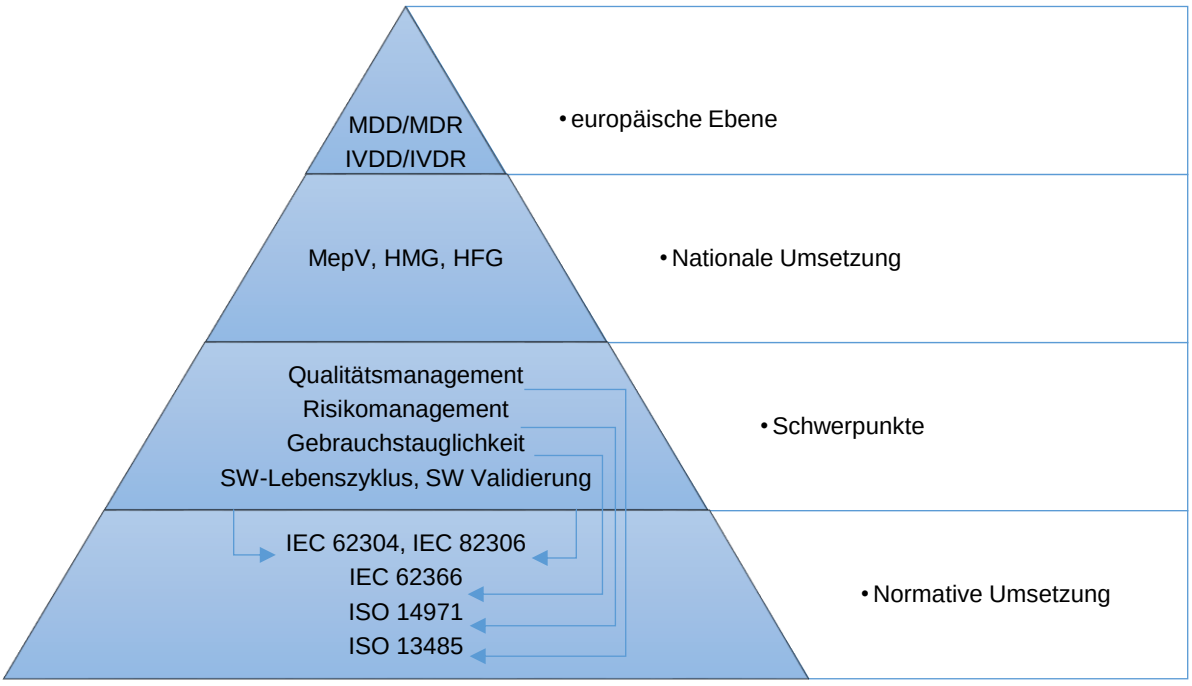

Abbildung 5: Zusammenhang Normen und Vorgaben (Quelle: ISS AG)

Normenbeschaffung

Normen sind urheberrechtlich geschützt und müssen von den Entwicklern auf eigene Kosten beschafft werden. Die Normen können z.B. beim SNV oder beim Beuth-Verlag online gekauft werden.

Normen werden regelmässig überarbeitet. Die neuen Versionen können grundlegende Änderungen der Anforderungen enthalten. Daher ist es wichtig, dass die für die Entwicklung verwendeten Normen regelmässig überwacht werden. Bei Änderungen muss zwingend eine Gap-Analyse durchgeführt werden, da Neuerungen beispielsweise ein neues Software-Release auslösen können.

2.9.1 ISO 13485:2016 Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke

ISO 13485, Qualitätsmanagementsystem

Die ISO 13485 definiert die medizinproduktspezifischen Anforderungen an ein Qualitätsmanagementsystem. Sie stellt eine spezifische Ausprägung der Qualitätsmanagementnorm ISO 9001 dar. In der ISO 13485 werden alle Anforderungen definiert, die das Qualitätsmanagement einer Medizinproduktefirma zu erfüllen hat, um sichere und zuverlässige Medizinprodukte zu gewährleisten. Die Zertifizierung wird durch eine Benannte Stelle vorgenommen. Alle Medizinprodukteherstellen (mit Ausnahme der Klasse I-Hersteller) müssen ISO 13485-zertifiziert sein, damit sie Medizinprodukte auf dem europäischen Markt in Verkehr bringen dürfen (Teil des Konformitätsbewertungsverfahrens).

2.9.2 IEC 62304:2016 Medizingeräte-Software - Software-Lebenszyklus-Prozesse

IEC 62304 Software-Lebenszyklus-Prozesse

Diese harmonisierte Norm definiert Anforderungen an den Lebenszyklus von Medizinprodukte-Software. Ursprünglich stammt die Norm aus dem Normenkreis der elektrischen Sicherheit (60601-X), sie ist aber auch bei eigenständiger Software, die als Medizinprodukt qualifiziert ist, anwendbar. Bei der Entwicklung von Software, die Teil eines Medizinprodukts ist oder bei Software, die selbst das Medizinprodukt darstellt, kommt die 62304 zum Einsatz. Die Norm 62304 ist also für Mobile Medical Apps anwendbar.

Ein wichtiger Teil der Norm ist der Software-Entwicklungsprozess:

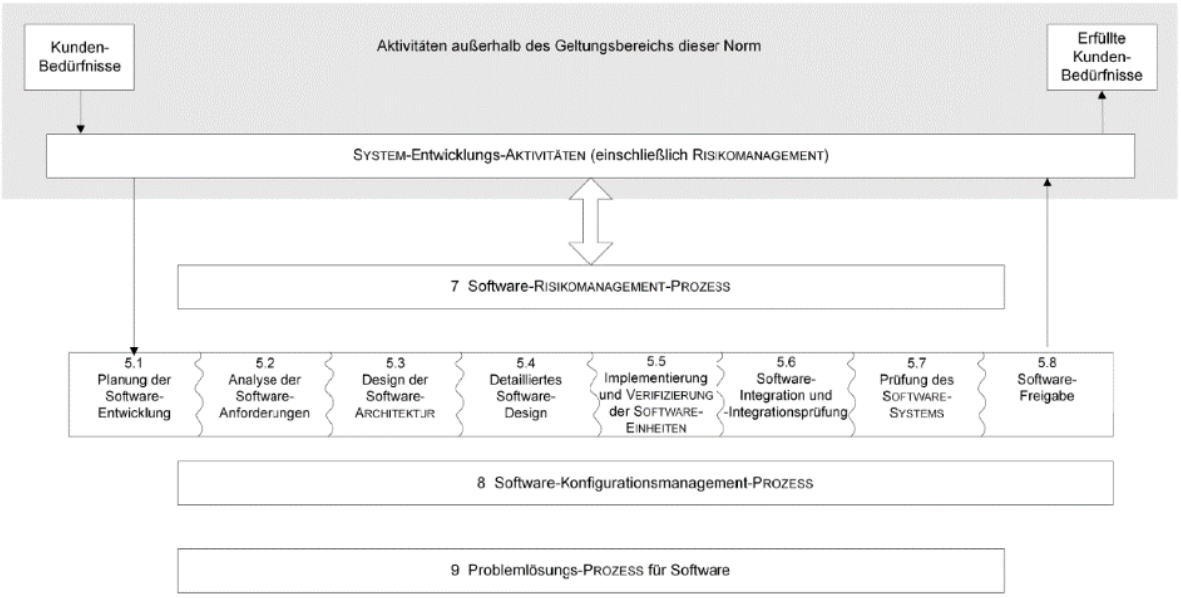

Abbildung 6: IEC 62304:2015 Figure 1 – Overview of software development PROCESSES and ACTIVITIES[1]

Der vorgeschlagene Prozess wird als grundlegender Entwicklungsprozess für Medizinprodukte-Software angesehen und stellt im Entwicklungsprozess sicher, dass die notwendigen Schritte frühzeitig und strukturiert geplant, durchgeführt und validiert werden.

[1] IEC 62301 ed 1.1 Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch

IEC 62366, Gebrauchstauglichkeit

2.9.3 EN IEC 62366:2008 Anwendung der Gebrauchstauglichkeit auf Medizinprodukte

Diese Norm beinhaltet die Gebrauchstauglichkeit von Medizinprodukten sowie deren Validierung und Verifizierung. Die IEC 62366 versteht unter Gebrauchstauglichkeit die *„Eigenschaft der Benutzer-Produkt-Schnittstelle, die die Effektivität, Effizienz, Lernförderlichkeit und Zufriedenstellung des Benutzers umfasst."* Laut MDD ist der Hersteller verpflichtet, dass sein Produkt möglichst anwenderfreundlich ist. Der Hersteller hat somit alle Risiken und Gefahren, die durch eine mangelnde Gebrauchstauglichkeit entstehen können, zu minimieren. Zudem müssen Vorwissen und die technischen Kenntnisse und Fertigkeiten des Anwenders in die Entwicklung miteinbezogen werden. Ein Beispiel dafür ist eine sehr kleine, schlecht leserliche Schrift auf einer für ältere Personen ausgelegten Einmalspritze. Die Norm hilft dem App-Entwickler zudem, seine Nutzergruppe im Auge zu behalten und sich möglicher Gefahren bei der Benutzung durch eine spezifische Patientengruppe bewusst zu werden.

ISO 14971, Risikomanagement

2.9.4 ISO 14971:2013 Anwendung des Risikomanagements auf Medizinprodukte

Die ISO 14971 beschäftigt sich mit dem Risikomanagement bei der Herstellung von Medizinprodukten. Medizinprodukthersteller müssen nachweisen, dass ihre Patientenrisiken beherrschbar sind. Die Norm fordert daher, dass eine Risikoanalyse zum betreffenden Produkt durchgeführt wird und die beschriebenen Risiken so weit wie möglich minimiert werden. Alle Restrisiken müssen zusätzlich dargestellt werden, um danach in der klinischen Bewertung nach ihrem Kosten/Nutzen-Verhältnis bewertet zu werden. Patientenrisiken können sich beispielsweise durch Sicherheitslücken beim Gebrauch mobiler Geräte ergeben. Hier muss anhand der Risikoanalyse die Möglichkeit eines Schadens sowie dessen Schweregrad eingeschätzt werden. In einem weiteren Schritt sind Massnahmen zu definieren, die dieses spezifische Risiko mindern (Cybersecurity, Security Updates, Bugfixes…). Dabei gilt es insbesondere zu beachten, dass ein Software-Update für ein App, die ein Medizinprodukt ist, deutlich aufwändiger ist als für eine „normale" App (Verifizierung, Validierung, Dokumentation, Information etc.).

2.9.5 IEC 82304-1:2016 Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit

IEC 82304-1
Health-Software

Die IEC 82304-1 wurde 2016 erstmals veröffentlicht, um bestehende Lücken zur 62304 zu schliessen. In den Anwendungsbereich der IEC 82304-1 fallen alle Software-Produkte und Apps, die auf allgemeinen Computersystemen, Handys und Tabletts eingesetzt werden und die dazu bestimmt sind, die Gesundheit oder die Pflege von individuellen Personen zu unterstützen, zu erhalten oder zu verbessern.
Diese Norm ist insbesondere für Validierung von Health-Software von Bedeutung und spielt auch für Entwickler ausserhalb der Medizinproduktebranche (z.B. Entwickler für Health/Wellbeing/Lifestyle. -Apps) eine wichtige Rolle.

3 MedTech und agile Entwicklung, geht das?

3.1 Das Wichtigste in Kürze

Auch MedTech-Anwendungen können agil entwickelt werden. Allerdings müssen gewisse Kompromisse gemacht werden. Die relevante Norm gibt Punkte vor, die berücksichtigt werden müssen. Kern des Kompromisses ist, dass an definierten Meilensteinen die relevante Dokumentation vervollständigt und freigegeben wird.

3.2 Agiler Entwicklungsprozess

Agile Entwicklung trotz IEC 62304

Software wird heute meist iterativ entwickelt. Das eher starre und sequenzielle V-Modell aus der Norm IEC 62304 steht zu agilen Methoden in einem gewissen Konflikt.

V-Modell

Das V-Modell sieht einen sequenziellen Entwicklungsprozess vor:

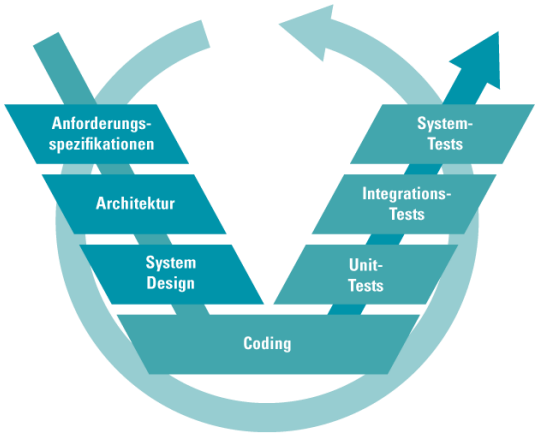

Abbildung 7: vereinfachtes V-Modell (Bild: ISS AG)

Ein Ausweg aus diesem Konflikt ist aber durchaus möglich. Es gilt zu beachten:

- das V-Modell als Dokumentenlandschaft verstehen und nicht als starren Entwicklungsablauf
- Softwareentwicklungsplan (insb. Dokumentenplan) bei Projektbeginn erstellen und freigeben.
    - Draft des Plans während des Projekts laufend anpassen (aber nicht bei jeder Änderung freigeben)
    - Freigabe des Plans nur bei wesentlichen Änderungen
- Fortlaufende Anpassung aller Dokumente, Anforderungen und Design müssen spätestens vor Prüfaktivitäten (Verifizierung) freigegeben werden.
- Reviews planen und regelmässig durchführen und dokumentieren.
- Für ein Release einen vollständigen und widerspruchsfreien Dokumentationszustand herstellen und prüfen (Reviews), vgl. dazu auch die entsprechende Checkliste.

3.3 Normative Einbettung

Technical Information Report

Es gibt keine normativen Vorgaben, die agile Programmierung für den Einsatz in der Medizintechnik regeln. Allerdings gibt es einen Technical Information Report der “Association for the Advancement of Medical Instrumentation (AAMI), der eine hohe Beachtung findet. Wir empfehlen, sich bei der Definition des eigenen Entwicklungsprozesses für SW-Entwicklung mit agilen Methoden an die Vorschläge des TIR45 zu halten. Der Report ist zahlungspflichtig.

3.3.1 Tool-Validierung

Validierung der Entwicklungstools

Die IEC 62304 schreibt ebenfalls eine Validierung der für die Entwicklung benutzten Tools vor. Auch hier gibt es von der AAMI einen technischen Report (TIR 36). Für die Validierung der Entwicklungstoolchain wird empfohlen, sich an diesen Report zu halten. Dieser Report ist zahlungspflichtig.

4 Cybersecurity (Datensicherheit)

4.1 Das Wichtigste in Kürze

Hersteller sind verpflichtet softwarespezifische Gefahren und Risiken zu betrachten, in der Risikoanalyse auszuweisen und entsprechende Massnahmen zur Risikominderung vorzunehmen. Voraussetzung für ein ausreichendes Sicherheitskonzept ist bereits beim Design erste Überlegungen und Anforderungen an die Sicherheit zu definieren. Wie potenzielle Gefahren und Risiken getestet werden müssen, ist nicht geregelt und muss an die jeweilige Software und deren Funktionen angepasst werden. Um Risiken, die zum Zeitpunkt der Entwicklung noch nicht bekannt sind, entgegenzuwirken, bleibt es ein andauernder Prozess. Zu den Pflichten des Herstellers gehören auch das Einführen eines Produktebeobachtungssystems und das Einbeziehen der so gewonnenen Erkenntnisse bei der Herstellung und Weiterentwicklung des Produkts.

Cybersecurity & Sicherheitsanforderungen an Medizinprodukte

Dank bilateraler Verträge hat die Schweiz das System der Konformitätsbewertung bzw. Zertifizierung der EU übernommen, das bedeutet, dass die Medizinprodukterichtlinie (MDD) (und in nicht allzu ferner Zukunft die Medizinprodukteverordnung) anwendbar ist. Aufgrund des von der MDD vorgegebenen, risikobasierten Entwicklungsansatzes bei Medizingeräten ist ein angemessenes Sicherheitskonzept für jedes Medizinprodukt nötig, wobei Software keine Ausnahme macht. Ganz im Gegenteil, da davon auszugehen ist, dass ein netzwerkfähiges Gerät in Kontakt mit Schadsoftware kommen wird, muss sichergestellt werden, dass dadurch kein Patienten- oder Bedienerrisiko entsteht. Dabei müssen softwarespezifische Gefahren und Risiken betrachtet werden und Hersteller von medizinischer Software sind verpflichtet, Patientenrisiken so gering wie möglich zu halten und entsprechende Massnahmen zu ergreifen. Die MDR stellt allgemein eine Verschärfung der Regulierung von Medizinprodukten (mit dem Ziel den Patienten zu schützen) dar, dabei wird erstmals auch medizinischer Software ein Artikel gewidmet. Artikel 11 ändert für Hersteller von medizinischer Software so einiges, da nun eine neue Begriffsdefinition von Software festgehalten ist und die neuen Klassifizierungsregeln die meisten Software-Produkte in eine höhere Risikoklasse einstufen. Höhere Risikoklasse bedeutet höhere regulatorische Anforderungen, die auch die Sicherheit und den Nachweis der Sicherheit betreffen werden. Bei der Zertifizierung von Software im oder als Medizinprodukt muss dokumentiert und nachgewiesen werden, das genügend Sicherheitsmassnahmen umgesetzt werden und somit sowohl die Leistung als auch der Schutz sensibler Daten gesichert sind.

Für Entwickler gilt es bereits beim Design erste Überlegungen und Anforderungen an die Sicherheit zu definieren. Im Entwicklungsprozess gibt es mehrere Anknüpfungspunkte für das Sicherstellen und Testen der Sicherheit:
-beim Definieren der *Device Requirements*
-beim Entwickeln der *Device Architektur*
-beim Erstellen der Risikoanalyse
-bei der Verifizierung und Validierung
-bei der Produktpflege/ *Sustaining Engineering* (Aktualisierungen, Bugfixes, etc.)

Sicherheit beginnt beim Design

Medizinische Software übernimmt heutzutage vielseitige Funktionen im oder als Medizinprodukt so z. B. die Steuerung komplexer Medizingeräte oder die Verarbeitung und Speicherung von Daten. So vielseitig die Funktionen, so zahlreich sind auch Risiken (und *Vulnerabilities*) und die Auswirkungen möglicher Fehlfunktionen bei programmierbaren Medizinprodukten. Gerade vernetzte Medizinprodukte sind anfällig für Manipulation und Fremdzugriff und der Schutz der Daten muss gewährleistet werden. Dies kann nur erreicht werden, wenn diese Punkte schon bei Konzept und **Design der Software** berücksichtigt werden. Je früher im Prozess Risikomanagement betrieben wird, desto einfacher und nachhaltiger ist das Sicherheitskonzept. Typische Punkte sind z. B.
-Vernetzung mit Netzwerken/anderen Geräten (Connectivity)
-Zugriffschutz und Berechtigungen
-Anmeldungen (Passwortrichtlinien, Entfernen von alten Accounts etc.)
-Automatisches Logoff aus Applikation
-Sicherheit Netzwerkkommunikation und Server
-Zugriffschutz auf Backups
-Datenverschlüsselung (müssen Daten verschlüsselt werden? Wenn ja, wie und wie wird Kommunikation mit weniger sicheren Verschlüsselungsstandards geregelt?)
-Datenarchivierung und Löschung
-Datenintegrität
-Aktualisierung der Software

Risikoanalyse

Verschiedene Faktoren sind für die Bestimmung der zu ergreifenden Massnahmen relevant, so gibt es zusätzlich zur Vorgabe eines Sicherheitskonzepts alle vorhersehbaren Risiken zu minimieren (oder zu eliminieren). Dabei ist speziell den spezifischen Patienten- und Bedienerrisiken Beachtung zu schenken. Diese müssen identifiziert

werden und technisch möglichen und den Risiken angebrachten Massnahmen gegenübergestellt werden. Hier bietet die Norm zur Risikoanalyse ISO 14971 Hilfestellung (s. Kapitel 2.8.4) um Risiken im Zusammenhang mit der Einsatzumgebung und der Zweckbestimmung zu bewerten. Das Erstellen der Risikomanagementanalyse bei Software ist ein wichtiger Schritt, um den Anforderungen an Sicherheit gerecht zu werden. Dabei werden Risiken nicht nur analysiert, sondern auch ausgewiesen, und Massnahmen betreffend ihrer Effektivität als Risikomassnahmen bewertet und definiert. *State of the Art* ist dabei ein entscheidender Faktor, welche Massnahmen technisch möglich sind; dies wird häufig auch aufgrund von Expertenwissen entschieden und ist nicht zwingend in Normen festgehalten. Die für die Herstellung von Software relevante Norm IEC 62304 (s. Kapitel 2.8.2) sowie IEC 82304 (s. Kapitel 2.9.5) müssen eingehalten werden. Die IEC 62304 wird zurzeit überarbeitet. Im aktuellen Draft sind Forderungen nach Sicherheitsmassnahmen erstmals explizit formuliert.

Verifizierung und Validierung

Wie potenzielle Gefahren und Risiken getestet werden, ist nicht strikt vorgegeben und muss an die jeweilige Software und deren Funktionen angepasst werden. Oft werden folgende Schritte für die Evaluierung der Sicherheit vorgenommen:
-Testen der Sicherheitsprotokolle
-Fuzz testing
-Testen der Software durch gezielte Angriffe von Experten

Sicherheit nach Markteinführung

Trotz aller möglichen Massnahmen ist eine 100-%-Sicherheit nicht zu erreichen. Pflichten für den Hersteller bestehen auch nach der Entwicklung der Software, so muss er angemessene Prozesse für sichere Updates bereitstellen und auf auftretende Sicherheitsrisikos reagieren können. Deshalb ist es entscheidend möglichst alle potenziellen Risiken während des Herstellungsprozesses zu identifizieren und zu kennen. Da es auch neue Risiken geben kann, die zum Zeitpunkt der Entwicklung noch nicht bekannt sind, bleibt es ein andauernder Prozess. Zu den Pflichten des Herstellers gehören auch das Einführen eines Produktebeobachtungssystems und das Einbeziehen der so gewonnenen Erkenntnisse bei der Herstellung und Weiterentwicklung des Produkts.

Gesetzliche Grundlagen

In der EU bestehen keine konkreten gesetzlichen Vorgaben betreffend Cybersecurity von Medizinprodukten und die Anforderungen sind im vorgegebenen, risikobasierten Entwicklungsansatz der

Richtlinien impliziert, da ein angemessenes Sicherheitskonzept verlangt wird. Sobald ein Notified Body involviert ist, wird dieser beurteilen, ob die vorgenommenen Massnahmen angemessen und ausreichend sind und diese Praxis wird unter der MDR strenger werden. Die MDD referenziert zudem die Norm IEC 62304, die das Thema Cybersecurity nur streift, aber als einzige Norm explizit aufgreift (zudem wird die neue Version voraussichtlich Anforderungen beinhalten).

Die FDA hat betreffend Cybersecurity mehrere Guidelines veröffentlicht, diese Dokumente sind zwar rechtlich nicht bindend, aber können bei der Entwicklung hilfreich sein. Unter anderem sind folgende Guidelines von Interesse:

Guideline	**Kommentar**
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Empfiehlt, dass Cybersicherheit Teil der Software-Validierung und des Software-Risikoprozesses sein soll. Definiert Consensus Standards aus anderen Bereichen welche angezogen werden können.
Postmarket Management of Cybersecurity in Medical Devices	Cybersecurity ist Teil des Risikoprozesses und des Post Market Managements
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Empfehlungen und Auslegung der FDA betreffend Cybersecurity / Sicherheits-Updates von off-the-shelf Software in Geräten; Verantwortlichkeiten, Validierung, etc.

Entwicklungen und Leitfäden in anderen Ländern:

Dass es sich beim Thema Cybersecurity und Datenschutz bei Medizinprodukten um ein aktuelles und noch nicht abschliessend geklärtes Thema handelt, zeigt sich auch durch die vielen Bemühungen der Staaten, diesen Bereich zu regeln und Expertenwissen zur Verfügung zu stellen.
So hat in Irland im Juni 2017 die Health Product Regulatory Authority einen Guide To Placing Medical Device Standalone Software on the Market herausgegeben, der sich auch mit Cybersecurity und Datenschutz beschäftigt.

Frankreich hat ein Expertenkomitee zum Thema Cybersecurity bei Medizinprodukten gegründet, das in Zukunft Guidelines und Dokumente als Hilfestellungen für Hersteller veröffentlichen wird: Création d'un comité scientifique sur la cybersécurité des logiciels dispositifs médicaux (ANSM).

Typische Überlegungen zur Sicherheit bei der Review von Software:

Review Topic	**Beschreibung**
SOUP	Enthält die Software oder das System SOUP (software of unknown provenance)? Identifikation der SOUP und der verwendeten Softwareversionen
Fixe Passwörter oder Schlüssel	Verwendet die Software fixe Passwörter oder Schlüssel, welche auf allen Geräten oder Installationen gleich sind?
Human Interface Benutzereingaben	Werden Benutzereingaben validiert und auf gültige Bereiche begrenzt? Sind gültige Bereiche definiert? Wurde dies getestet?
Machine Interface Netzwerk	Ist die Kommunikation gegen mutwillige oder versehentliche Eingriffe geschützt?
Machine Interfacee Dateiformate	Sind Datenformate klar definiert? Sind Daten gegen Änderungen geschützt?

Threat-Model

Das Threat-Model ist ein möglicher Ansatz mit den Sicherheitsanforderungen für medizinische Software umzugehen. In diesem Model werden sowohl mögliche Objekte, die es durch Massnahmen zu schützen gilt, als auch mögliche Angreifer, die Patienten- oder Bedienerrisiken und Angriffsvektoren definiert.
Folgende Tabellen sind beispielhaft für (ein unvollständiges) Threat-Model zu betrachten:
Zu schützende Objekte oder Prozesse

Schutzobjekt	**Kommentar**
Patientendaten	Relevant für Software, die Patientendaten verarbeitet/ auswertet/speichert
Geschäftsdaten	Relevant für Software, die Geschäftsdaten verarbeitet/ auswertet/speichert
Integrität des Gerätes/Systems	DOS/Kryptotrojaner/Erpressung

Betrieb des Gerätes/Systems	DOS/Kryptotrojaner/Erpressung

Angreifer	Motivation	Wahrscheinlichkeit
Aktivist	Ideologisch	zu definieren
Hacker	Spass	
Hacker	Kommerziell	
Konkurrent	Kommerziell	
Kriminelle	Kommerziell	
..		

Angreifer

Vektor	**Beschreibung**
Physikalische Geräteschnittstelle	USB, Seriell, Netzwerk
Logische Geräteschnittstelle	Human Interface, Machine Interface
..	

Angriffsvektoren

Es gibt zudem verschiedene Sicherheitskonzepte und Prinzipien, die zur Erfüllung von Sicherheitsanforderungen im Zusammenhang mit Software angewendet werden können:

Sicherheitskonzepte

Konzept	**Beschreibung**
Defense in depth	Sicherheitsmassnahmen werden nicht nur an den Grenzen des Systems implementiert, sondern auch innerhalb des Systems.
Least privilege	Ein Prozess oder eine Softwarekomponente sollte nur so viele Rechte und Berechtigungen haben wie nötig ist, um die definierte Aufgabe zu erfüllen.
Minimization	Auf einem Gerät laufen nur Software und Dienste die benötigt werden; dies führt zu einer Reduktion der Angriffsfläche.
Compartementalization	Verschiedene Dienste/Software/Applikationen laufen voneinander abgeschottet und kommunizieren nur über definierte Schnittstellen. Geräte enthalten keine Informationen welche direkt für den Angriff auf andere Geräte verwendet werden können (z.B. Fixe Passwörter oder Schlüssel).
Audit Trail	Aktivitäten werden geloggt

Angepasst aus Fundamental Security Concepts

5 Rechtsgrundlage Datenschutz und -sicherheit in der Schweiz

5.1 Das Wichtigste in Kürze

Für die Bearbeitung von Personendaten im Bereich von Gesundheits-Apps gelten aus datenschutzrechtlicher Sicht hohe bis sehr hohe Anforderungen, da es sich dabei um besonders schützenswerte Daten handelt. Hersteller sind verpflichtet, die gesetzlichen Vorgaben einzuhalten und mit technischen und organisatorischen Massnahmen für eine risikogerechte Datensicherheit zu sorgen. Werden Personendaten aus der EU verarbeitet, müssen zudem die strengeren Vorgaben der EU beachtet werden.

5.2 Anwendbarkeit Datenschutzgesetzgebung

Gesetzgebung und Anwendungsbereich

Die Datenschutzgesetzgebung besteht aus dem Datenschutzgesetz und der Datenschutzverordnung und leitet sich aus dem Grundrecht auf informationelle Selbstbestimmung ab. Sie gelangt immer dann zur Anwendung, wenn eine **«Bearbeitung (a) von Personendaten (b)»** stattfindet:

(a) Der Begriff **«Bearbeiten»** umfasst praktisch jeden Umgang mit Personendaten – z.B. das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben (Zugänglichmachen), Archivieren oder Vernichten von Daten. Ob die Datenbearbeitung elektronisch oder in Papierform erfolgt, spielt keine Rolle. Ebenfalls spielt es bei einer elektronischen Bearbeitung keine Rolle, mit welchen Mitteln oder Diensten die Bearbeitung stattfindet. Viele Bearbeitungen, die elektronisch erfolgen, umfassen Profiling-Aktivitäten. Profiling ist die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten. Das Ziel von Profiling-Aktivitäten besteht darin, z.B. die Gesundheit, die Arbeitsleistung oder die wirtschaftlichen Verhältnisse einer Person zu analysieren oder vorauszusagen. Auch Profiling-Aktivitäten sind vom Begriff des Bearbeitens erfasst.

(b) «Personendaten» sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bestimmbar ist eine Person, wenn sie sich mittels Zuordnung zu einer Kennung wie z.B. einem Namen oder einer Nummer identifizieren lässt. Die Datenschutzgesetzgebung unterscheidet zwei Arten von Personendaten:

- **Normale Personendaten** – z.B. Name, Anschrift, Geburtsdatum
- **Besonders schützenswerte Personendaten** – z.B. Gesundheitsdaten, genetische und biometrische Daten, Daten über religiöse, weltanschauliche oder politische Ansichten, Daten über Massnahmen der sozialen Hilfe

Für die Bearbeitung von besonders schützenswerten Personendaten und Profiling-Aktivitäten gelten höhere Bearbeitungsanforderungen als für die Bearbeitung normaler Personendaten.

Datenschutz im Bereich von medizinischen Apps

Im Rahmen von Gesundheits-Apps findet eine Bearbeitung von besonders schützenswerten Personendaten in Form von Gesundheitsdaten und je nach Sachlage auch von genetischen oder biometrischen Daten statt. Zudem findet die Bearbeitung verbreitet in Form von Profiling-Aktivitäten statt. Entsprechend gelten für die Bearbeitung von Personendaten im Bereich von Gesundheits-Apps aus datenschutzrechtlicher Sicht hohe bis sehr hohe Anforderungen.

Besonders schützenswerte Daten

Die Datenschutzgesetzgebung enthält mehrere Vorgaben, die es bei der Bearbeitung von besonders schützenswerten Personendaten und Profiling-Aktivitäten zwingend zu beachten gilt. Nachfolgend finden sich die Wichtigsten erklärt:

Einwilligung oder gesetzliche Grundlage

Die Bearbeitung von Personendaten setzt entweder die Einwilligung der Person über die Daten bearbeitet werden oder eine gesetzliche Grundlage, die eine entsprechende Datenbearbeitung vorsieht, voraus. Basiert die Datenbearbeitung auf der Einwilligung, ist die Einwilligung nur gültig, wenn sie folgende Voraussetzungen erfüllt: Sie erfolgt für einen bestimmten Bearbeitungszweck oder mehrere bestimmte Bearbeitungszwecke sowie nach angemessener Information, freiwillig, eindeutig und ausdrücklich.

Datenbearbeitungen im Rahmen von Gesundheits-Apps basieren in der Regel auf der Einwilligung der Nutzer. Eine solche gilt es somit einzuholen. Damit die Einwilligung gültig ist, müssen die Nutzer in einen bestimmten Bearbeitungszweck oder mehrere bestimmte Bearbeitungszwecke einwilligen. Zudem muss die Einwilligung freiwillig (ohne Druck), eindeutig (zweifelsfrei) und ausdrücklich (idealerweise schriftlich und damit nachweisbar) erfolgen.

Zweckbindung

Es muss für die Personen, über die Daten bearbeitet werden, bei der Erhebung der Daten klar sein, für welche Zwecke die Daten erhoben werden. Eine spätere Änderung des Zwecks ist nur zulässig, wenn die betroffenen Personen in die Zweckänderung einwilligen.

Gibt der App-Anbieter als Zweck für die Datenbearbeitung die Nutzung der App an, darf er die erhobenen Daten nicht zu Werbezwecken verwenden oder an einen Dritten weitergeben – ausser die Nutzer stimmen der Verwendung ihrer Daten zu diesen weiteren Zwecken zu.

Datensparsamkeit (Verhältnismässigkeit)

Es dürfen jeweils nur so viele Daten erhoben und bearbeitet werden, wie dies zur Erreichung des bei der Datenerhebung angegebenen Zwecks notwendig ist. Will die datenbearbeitende Person mehr Daten erheben bzw. bearbeiten, darf sie das nur tun, wenn die von der Bearbeitung Betroffenen in diese weitere Datenerhebung bzw. Datenbearbeitung eingewilligt haben. Benötigt die datenbearbeitende Person Daten nicht mehr, ist sie verpflichtet, die Daten zu löschen oder zu anonymisieren.

Ein App-Anbieter darf von den Nutzern nur so viele Daten erheben und bearbeiten, wie er zur Erfüllung des angegebenen Zwecks (z.B. der Nutzung der App) zwingend braucht. Will er mehr Daten erheben bzw. bearbeiten, darf er dies nur tun, wenn die Nutzer in diese erweiterte Datenbearbeitung eingewilligt haben. Benötigt der App-Anbieter die Daten nicht mehr, ist er verpflichtet, diese zu löschen oder zu anonymisieren.

Gewährleistung der Datensicherheit

Die Verarbeitung von Personendaten erfolgt nur dann datenschutzkonform, wenn durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit garantiert wird.

Hersteller und Anbieter von Apps sind verpflichtet, durch geeignete technische und organisatorische Massnahmen für eine risikogerechte Datensicherheit zu sorgen. Da im Rahmen von Gesundheits-Apps besonders schützenswerte Personendaten bearbeitet werden und Profiling-Aktivitäten stattfinden, besteht ein überdurchschnittlich hohes Risiko für die Datensicherheit. Die eingesetzten technischen und organisatorischen Massnahmen müssen deshalb besonders hohe Anforderungen erfüllen.

Gewährleistung der Betroffenenrechte

Die Datenschutzgesetzgebung sieht für die von der Datenbearbeitung betroffenen Personen mehrere Rechte vor (Betroffenenrechte): Die Betroffenen sind berechtigt, vom Datenbearbeiter jederzeit darüber Auskunft zu verlangen, welche Daten er über sie bearbeitet. Enthalten die bearbeiteten Daten Fehler, sind die Betroffenen berechtigt, vom Datenbearbeiter eine Berichtigung der Daten zu verlangen.

Damit die Nutzer einer App ihre Betroffenenrechte wahrnehmen können, müssen sie darüber informiert sein, wer für die Datenbearbeitung verantwortlich ist – dies bedeutet, sie müssen eine Ansprechstelle haben, bei der sie ihre Rechte geltend machen können.

Notwendigkeit zur Beachtung der EU-Datenschutzgesetzgebung

Datenschutz auf EU-Ebene

Im Weiteren ist darauf hinzuweisen, dass am 25. Mai 2018 die neue EU-Datenschutzgesetzgebung in Kraft tritt. Diese gilt zwar primär für Datenbearbeitungen innerhalb der EU, sie kann aber ausnahmsweise auch für einen Datenbearbeiter, der sich ausserhalb der EU befindet, gelten. Dies ist der Fall, wenn ein Datenbearbeiter, Personen, die sich in der EU befinden, Waren oder Dienstleistungen anbietet und über die Personen, denen er die Waren oder Dienstleistungen anbietet, Personendaten bearbeitet.

Bietet ein App-Entwickler mit Sitz in der Schweiz seine App auch Personen, die sich in der EU befinden an und bearbeitet er in diesem Zusammenhang über diese Personen Daten, findet auf ihn die EU-Datenschutzgesetzgebung Anwendung.

Ein Bewusstsein über diesen Umstand ist deshalb notwendig, weil die EU-Datenschutzgesetzgebung teilweise strengere Bearbeitungsvoraussetzungen als die schweizerische Datenschutzgesetzgebung enthält und bei Verstössen hohe Geldbussen vorsieht (bis zu einem zweistelligen Millionenbetrag). Werden somit Apps auch in der EU angeboten und findet über die Personen, denen die App in der EU angeboten werden, eine Bearbeitung von Personendaten statt, empfiehlt sich dringend eine vertiefte rechtliche Abklärung der Sachlage. Die EU hat einen Leitfaden zur Entwicklung von Gesundheits-Apps entwickelt. Der Leitfaden sowie weiterführende Informationen finden sich hier.

Analyse im Einzelfall immer nötig

Abschliessend ist darauf hinzuweisen, dass diese Ausführungen eine vertiefte Analyse des Einzelfalls nicht zu ersetzen vermögen. Je nach Sachlage empfiehlt sich die Beiziehung eines Datenschutzspezialisten.

MedTech Glossar für den App Entwickler

Gesetze, Normen und Standards

Norm Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke	ISO 13485
Norm Medizingeräte-Software - Software-Lebenszyklus-Prozesse	IEC 62304
Norm Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit	IEC 82304-1
Norm Anwendung des Risikomanagements auf Medizinprodukte	IEC 14971
aktuell gültige europäische Richtlinie für Medizinprodukte	MDD
ab 2020 gültige europäische Medizinprodukteregulierung	MDR
Medizinprodukteverordnung: gesetzliche Bestimmungen für Medizinprodukte von der Schweiz	MepV
Heilmittelgesetz: Bundesgesetz über Heilmittel und Medizinprodukte Text	HMG
Humanforschungsgesetz: Bundesgesetz über die Forschung am Menschen	HFG
Harmonisierte Standards	List of harmonized standards

6.2 Behörden, Vereinigungen etc.

schweizerisches Heilmittelinstitut, Zulassungs- und Kontrollbehörde für Heilmittel in der Schweiz	Swissmedic
International Medical Device Regulators Forum	IMDRF
Beispiel einer Benannten Stelle	TüV Süd
Notified Body Operations Group	NBOG

New Approach Notified and Designated Organisations	NANDO
The Medicines and Healthcare Products Regulatory Agency (UK)	MHRA
Bundesamt für Arzneimittel und Medizinprodukte (Deutschland)	BfArM

6.3 Wichtige Begriffe

Medizinprodukte zur medizinischen Laboruntersuchung von aus dem Körper stammenden Proben (**I**n-**V**itro-**D**iagnostika)	IVD
Internationale Organisation für Normung, Internationale Normenorganisation für alle Bereiche ausser Telekommunikation sowie Elektronik und Elektrotechnik	ISO
International **E**lectrotechnical **C**ommission, Normenorganisation im Bereich Elektronik und Elektrotechnik (z.B. IEC 60601-X)	IEC
Aktive **i**mplantierbare Medizinprodukte (**M**edical **D**evice) z.B. Herzschrittmacher	AIMD
Unique **D**evice **I**dentifier, System zur einheitlichen Produkteidentifizierung zur Sicherung der Verfolgbarkeit eines Produktes. Auch eine Software/App, die ein Medizinprodukt ist, muss künftig einen UDI haben.	UDI
Post **M**arket **S**urveillance (Marktüberwachung), systematische Informationssammlung und Auswertung über sich bereits im Markt befindliche Produkte um frühzeitig Korrektur- und Vorbeugungsmassnahmen herzuleiten, die das Risiko eines Produkts zu senken	PMS
Zertifizierungsweg, durch den der Hersteller ausweisen kann, dass sein Produkt die grundlegenden Anforderungen erfüllt und somit die erforderlichen EU-Richtlinien erfüllt	Konformitätsbewertungsverfahren
Minimalforderungen bezüglich Sicherheit und Leistung, die ein Medizinprodukt erfüllen muss. Vgl. Annex 1 der MDD	Grundlegende Anforderungen

7 Wichtige Ressourcen, Leitfäden etc.

Leitfaden zur Medizinprodukte-Regulierung	Leitfaden Swissmedic
Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide“)	Blueguide
MEDDEV-Dokumente	Guidance documents MEDDEV
Auflistung aller Benannten Stellen mit Akkreditierung nach 93/42/EEC Medical devices	Liste der Benannten Stellen
Schweizer Normenverband	Swiss Standards SNV
Leitfaden des MHRA	Is your app a medical device? (MHRA)
BfArM Auflistung zur Definition von Medizinprodukten	Was zählt zu Medizin-produkten?
BfArM Information zum Inverkehrbringen von Medizinprodukten	Im Überblick: Inver-kehrbringen von Me-dizinprodukten
Einschätzung, Klassifizierung und Abgrenzung durch das BfArM	Orientierungshilfe Medical Apps

7.1 Links, Blogs etc. von privaten Anbietern

Medizinprodukteblog *medicaldeviceslegal.com* zu allgemeinen wie auch softwarespezifischen Themen (z.B. Implementing Medical Device Cybersecurity: A Two-Stage Process oder The new General Data Protection Regulation impact on medical devices industry)	medicalesdeviceslegal
Blog mit Fokus auf digitaler Gesundheit	http://www.mobihealth-news.com/
Dienstleister mit Fokus auf Medizinprodukten, die Software enthalten	Johner Institut
Newsportal mit Fokus auf MedTech und neue Technologien	https://www.medgadget.com/