Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

eHealth Suisse

Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer

Praktische Hinweise

Bern, 7. April 2022

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

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

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 Inverkehrbringen 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, wann 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 vier 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 Apps, die als medizinische Software zu den Medizinprodukten zählen.

2 Grundlagen

2.1 Das Wichtigste in Kürze

Die Definition von Medizinprodukten ist gesetzlich in der schweizerischen Medizinprodukteverordnung MepV festgelegt und entspricht jener der europäischen Verordnung über Medizinprodukte MDR. 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. Zusätzlich zur Definition gibt es weitere Dokumente, die zur Entscheidungshilfe bei der Zuordnung zu Medizinprodukten bei Software dienen können (allen voran MDCG 2019-11). 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 Medizinprodukt

Die schweizerische Medizinprodukteverordnung definiert in Artikel 3 Medizinprodukte wie folgt:

Als Medizinprodukte gelten Instrumente, Apparate, Geräte, Software, Implantate, Reagenzien, Materialien oder andere Gegenstände:

a. die dem Hersteller zufolge für Menschen bestimmt sind;
b. deren bestimmungsgemässe Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann; und
c. die allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen:
    1. Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
    2. Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,

3. Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
4. Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper – auch aus Organ-, Blut- und Gewebespenden – stammenden Proben.

Als Medizinprodukte gelten ebenfalls:

a. Produkte zur Empfängnisverhütung oder -förderung;
b. Erzeugnisse, die speziell für die Reinigung, Desinfektion oder Sterilisation von Medizinprodukten bestimmt sind.

Definition Zubehör

Zubehör eines Medizinprodukts ist ein Gegenstand, der an sich kein Medizinprodukt ist, aber vom Hersteller dazu bestimmt ist, zusammen mit einem oder mehreren bestimmten Medizinprodukten verwendet zu werden, und:

a. der speziell dessen oder deren Verwendung gemäss seiner oder ihrer Zweck-bestimmung ermöglicht; oder
b. b. mit dem die medizinische Funktion des Medizinprodukts bzw. der Medizinprodukte im Hinblick auf dessen oder deren Zweckbestimmung gezielt und unmittelbar unterstützt wird.

Zubehör zu Medizinprodukten unterliegt ebenfalls der Medizinprodukteverordnung.

Klassische Medizinprodukte und IVD

Medizinprodukte werden weiter unterteilt in:

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

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.

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

Infovideos Swissmedic

- "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 Europa

Der freie Warenverkehr in Europa (New 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.

Auf europäischer Ebene sind Medizinprodukte aktuell durch zwei Verordnungen geregelt:

- Verordnung (EU) 2017/745 über Medizinprodukte
- Verordnung (EU) 2017/746 über In-vitro-Diagnostika

Im Mai 2017 traten die neuen Verordnungen über Medizinprodukte (MDR) und In-vitro-Diagnostika (IVDR) in Kraft. Die MDR löste die Richtlinien MDD und AIMD am 26. Mai 2021 ab, die IVDR wird am 26. Mai 2022 die IVDD ersetzen.

2017/745 (MDR)

2017/746 (IVDR)

Die neuen europäischen Medizinprodukte- und IVD-Verordnungen bedeuten für die Wirtschaftsakteure (Hersteller, Importeure, Distributoren, etc.) grosse Umstellungen und Herausforderungen. Auch Produkte, die sich unter der alten Regulierung bereits auf dem Markt befunden haben, müssen unter der MDR und IVDR neu zertifiziert werden (kein grandfathering). Die MDR und IVDR führen neue Klassifizierungsregeln (im Falle der IVDR ein komplett neues Klassifizierungssystem) ein und die Anforderungen an klinische Daten sowie Post Market Surveillance etc. sind beträchtlich gestiegen.
Zu den wichtigsten Änderungen gehören:

- Die technische Dokumentation muss wesentlich detaillierter erstellt werden.
- Alle Medizinprodukte müssen den UDI=Unique Device Identifier aufweisen.

- Jede Firma muss eine ‚person responsible for regulatory compliance (PRRC)' bestimmen, die über qualifiziertes Fachwissen auf dem Gebiet der Medizinprodukteregulierung verfügt.
- Die klinischen Bewertungen werden detaillierter verlangt, wobei auch PMS Daten bei einer Aktualisierung miteinbezogen werden müssen.
- Es gibt neue Klassifizierungsregeln in der MDR (z.B. Nanotechnologie, Software, etc.) respektive ein neues regelbasiertes Klassifizierungssystem in der IVDR.
- Die Klassifizierung einiger Produkte ändert sich ebenfalls (z.B. werden viele Software-Produkte von Klasse I zu Klasse IIa oder höher hochgestuft).

2.4 Gesetzliche Grundlagen in der Schweiz

Die wichtigsten Rechtsgrundlagen in der Schweiz sind:

- Bundesgesetz über Arzneimittel und Medizinprodukte
- die Medizinprodukteverordnung MepV
- die kommende Verordnung über In vitro Diagnostika (IvDV)
- das Bundesgesetz über die Forschung am Menschen
- die Verordnung über klinische Versuche in der Humanforschung

Heilmittelgesetz HMG
Medizinprodukte-verordnung MepV

Die MepV wurde im Zuge der Einführung der neuen Medizinprodukte-Regulierung in Europa überarbeitet und der MDR weitestgehend angepasst. Die neue MepV ist seit dem 26. Mai 2021 in Kraft. Die MepV nimmt in weiten Teilen direkten Bezug auf die MDR und die Anforderungen an Produkte und Wirtschaftsakteure (Hersteller, Importeure, Distributoren, Bevollmächtigte) sind grösstenteils identisch mit denen der MDR.

Die ebenfalls unter der alten MepV regulierten Medizinprodukte für die In vitro Diagnostika IVD werden neu eine eigene Verordnung erhalten (IvDV). Die IvDV orientiert sich an der europäischen IVDR. Bis zum Inkrafttreten der IvDV am 26. Mai 2022 gilt für IVD Produkte weiterhin die alte MepV.

Die Schweiz als Drittstaat im Sinne der MDR

Unter den alten Regulierungen (europäische MDD und alte Schweizer MepV) hatten Schweizer Hersteller dank bilateraler Verträge direkten Zugang zum europäischen Markt. Medizinprodukte, die in der Schweiz in Verkehr gebracht wurden, konnten ohne weitere Anforderungen auch in Europa vertrieben werden. Seit der Einführung der

MDR und der neuen MepV gilt die Schweiz jedoch als Drittstaat im Sinne der MDR und der Zugang zum europäischen Markt ist für Schweizer Hersteller erschwert. Mehr dazu in Kapitel 2.9.6.

Für Medizinprodukte in der Schweiz ist also die MepV (und ab dem 26. Mai 2022 die IvDV) geltend. Dieser Leitfaden nimmt jedoch in erster Linie auf die MDR Bezug. Da sich die MepV und MDR weitestgehend entsprechen und die MepV direkten Bezug zur MDR nimmt, sind die vorliegenden Informationen auch für die MepV gültig. Medizinprodukte von Schweizer Herstellern, die CE Zertifiziert in der EU auf den Markt gebracht wurden, können ohne Einschränkung auch in der Schweiz vertrieben werden.

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.

MDCG

Die ausführlichste Entscheidungshilfe, ob es sich bei einer Standalone Software um ein Medizinprodukt handelt, bietet der MDCG 2019-11 Leitfaden.

Die Medical Device Coordination Group MDCG ist ein von der MDR und IVDR gefordertes Expertengremium, welches sich aus Mitgliedern aus allen EU-Mitgliedstaaten zusammenstellt. Verschiedene Arbeitsgruppen der MDCG erarbeiten unter anderem so genannte MDCG-Dokumente als Hilfestellungen. Die MDCG-Dokumente sind rechtlich nicht bindend, geben aber Leitlinien und Hilfestellung bei der Interpretation der MDR und IVDR.
Für Standalone Software bietet die MDCG 2019-11Kriterien und Beispiele für die Einstufung von eigenständiger Software als mögliches Medizinprodukt nach der MDR und IVDR (siehe Kapitel 4.2.2).

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

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 veröffentlichte dazu Entscheidungen betreffend Borderline-Produkten im sogenannten Borderline Manual. Obschon sich die Entscheidungen in diesem Manual nur auf die MDD und nicht auf die MDR beziehen sind sie für die Auslegung der MDR weiterhin interessant, da sich die Definition eines Medizinprodukts nicht signifikant geändert hat. Die letzte Fassung des Manuals enthält verschiedene Entscheidungsbeispiele zu medizinischen Apps. Das Borderline Manual wird auch unter den neuen Regulierungen weitergeführt.

2.6 Meine Software ist kein Medizinprodukt. Was nun?

Kein Medizinprodukt

Wenn eine Software die Definition eines Medizinprodukts nicht erfüllt und aufgrund des MDCG-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

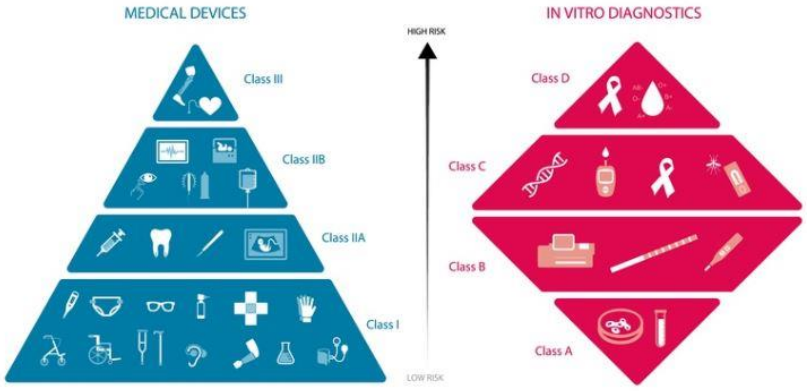

Abbildung 1 Risikoklassen MD und IVD EU (Quelle: MedTech Europe)

Risikoklassen MD

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

Risikoklasse	*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 2 Verordnung (EU) 2017/745 über Medizinprodukte Artikel 51

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:

Risiko-klasse	*Anhang II Liste A (hoch kritische IVDs)*	*Anhang II Liste B (kritische IVDs)*	*Produkte zur Eigenanwendung*	*Sonstige*
*Neu nach IVDR**	*D*	*C*	*B*	*A*
Beispiele	*Blutgruppen, HIV, Hepatitis*	*Infektionskrankheiten, Zytomegalovirus, Chlamydien*	*Schwangerschaftstest*	*Laborgerät*

Abbildung 3 Richtlinie 98/79/EG über In-Vitro-Diagnostika Artikel 9 Anhang II

* 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 CH- respektive 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 oder der Türkei akkreditiert ist und die jeweilige Produktgruppe in ihrem Scope hat. Die Schweiz verfügt über keine nach MDR akkreditierte Benannte Stelle. Schweizer Hersteller müssen also auf eine Benannte Stelle in der EU zurückgreifen wenn sie ihre Produkte auch auf den europäischen Markt bringen wollen. Produkte, die in der EU auf den Markt gebracht wurden und ein CE-Zeichen tragen, dürfen auch in der Schweiz vertrieben werden.

NANDO
NBOG

Informationen zu den Benannten Stellen finden sich im Informationssystem NANDO (New Approach Notified and Designated Organisations). Vorgaben und Verfahren zu Konformitätsbewertungen 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 (IVDD) und Produkte zur Eigenanwendung. Unter der kommenden IVDR muss ein deutlich grösserer Teil von IVD Produkten durch eine Benannte Stelle zertifiziert werden

Der Hersteller ist dabei selbst verantwortlich, dass seine Produkte die grundlegenden Sicherheits- und Leistungsanforderungen sowie die notwendigen CH- respektive EU-Richtlinien erfüllen.

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

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

CE mit Benannter Stelle

Eine Bewertung und periodische Überprüfung durch eine Benannte Stelle ist für folgende Produkte vorgeschrieben:

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

- In-vitro-Diagnostika der Klassen B, C und D nach der kommenden Verordnung (EU) 2017/746 (IVDR)

Abhängig von der Klassifizierung und Zweckbestimmung des Produkts 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 und der Hersteller erhält ein entsprechendes CE-Zertifikat. Der Hersteller kann seine Produkte nun konform in Verkehr bringen.

Konformitätsbewertungsverfahren

Wie bereits erwähnt, unterscheiden sich die Konformitätsbewertungsverfahren nach Risikoklasse. Der TüV Süd hat die 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 45020 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 (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 ein Produkt nach harmonisierten Normen hergestellt, so geht man automatisch von einer Erfüllung dieser wesentlichen Anforderungen aus (Konformitätsvermutung). Harmonisierte Normen sind im Amtsblatt der Europäischen Union veröffentlicht.

Für die MDR hat die EU Kommission einen Normungsauftrag an CEN und Cenelec gestellt der die zu harmonisierenden Normen auflistet. Bisher wurden davon erst wenige Normen für die MDR harmonisiert. Bis die Harmonisierung abgeschlossen ist können Hersteller zur Identifikation anwendbarer Normen auf den Normungsauftrag zurückgreifen.

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, das Produkt anwenderfreundlicher zu machen, z.B. durch Berücksichtigung der technischen Kenntnisse oder des Fachwissens des Anwenders, 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:

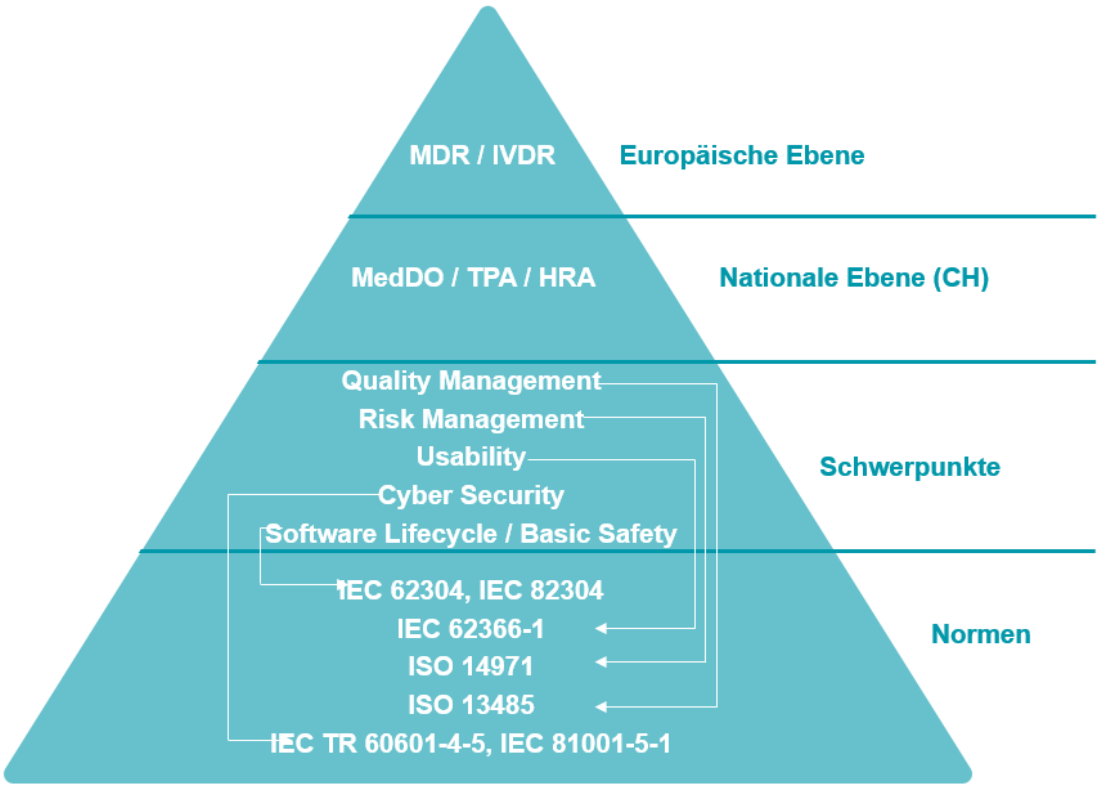

Abbildung 4: Zusammenhang Normen und Vorgaben (Quelle: ISS AG)

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 Qualitätsmanage-

ment einer Medizinproduktefirma zu erfüllen hat, um sichere und zuverlässige Medizinprodukte zu gewährleisten. Die Zertifizierung wird durch eine Benannte Stelle vorgenommen. Alle Medizinprodukteheresteller (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 62304:2006/Amd1:2015 Medizingeräte-Software - Software-Lebenszyklus-Prozesse

IEC 62304 Software-Lebenszyklus-Prozesse

Diese Norm definiert Anforderungen an die Prozesse im Lebenszyklus von Medizinprodukte-Software (Entwicklung, Wartung, Problemlösung, Risikomanagement). Ursprünglich wurde sie für Software, die Teil eines Medizingerätes ist (Embedded Software) entwickelt. In Kombination mit IEC 82304 findet sie auch für Software, welche selbst ein Medizinprodukt ist Anwendung (Standalone Software). Die Norm IEC 62304 ist also für Mobile Medical Apps anwendbar.

Ein wichtiger Teil der Norm ist der Software-Entwicklungsprozess:

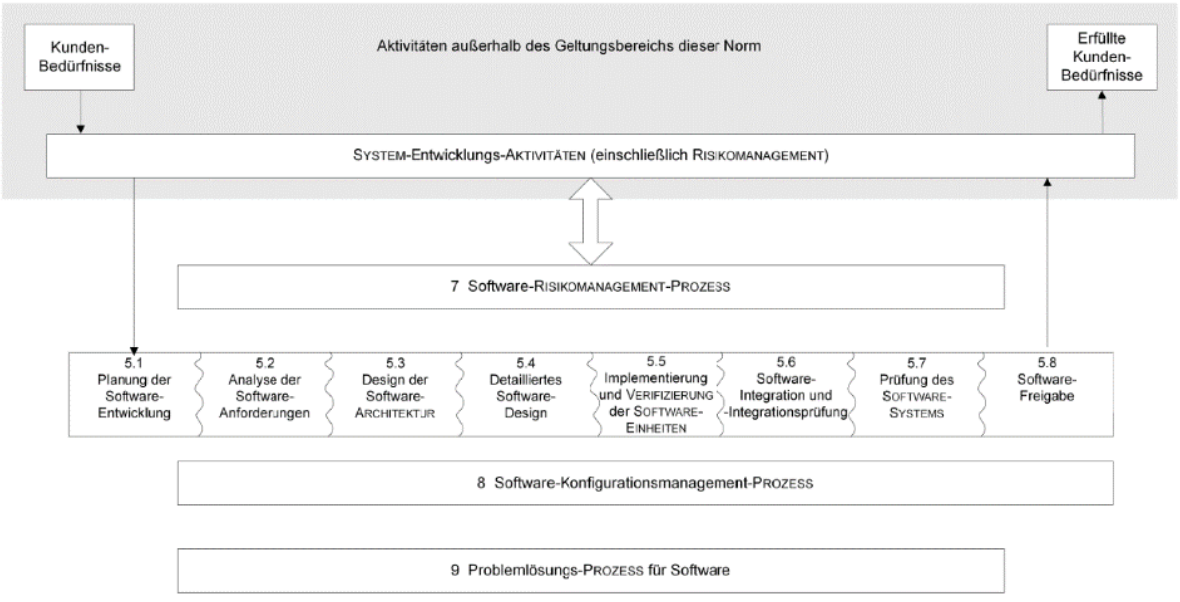

Abbildung 5: IEC 62304:2006+AMD1:2015 Figure 1 – Overview of software development PROCESSES and ACTIVITIES [translated]

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 verifiziert werden.

Die Entwicklung nach IEC 62304 lässt sich im Prinzip mit agilen Entwicklungsmethoden umsetzen, hat aber in der Praxis gewisse Anforderungen, welche sich nur schwer mit einem rein agilen Prozess erfüllen lassen.

2.9.3 IEC 62366-1:2015/Amd1:2020 Anwendung der Gebrauchstauglichkeit auf Medizinprodukte

IEC 62366, Gebrauchstauglichkeit

Diese Norm betrifft die Gebrauchstauglichkeit von Medizinprodukten sowie deren Verifizierung und Validierung. Die IEC 62366 versteht unter Gebrauchstauglichkeit die *Eigenschaft der Benutzer-Produkt-Schnittstelle, die die Effektivität, Effizienz, Lernförderlichkeit und Zufriedenstellung des Benutzers umfasst.* Laut MDR 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.

2.9.4 ISO 14971:2019 Anwendung des Risikomanagements auf Medizinprodukte

ISO 14971, Risikomanagement

Die ISO 14971 beschäftigt sich mit dem Risikomanagement bei der Entwicklung, Herstellung und Anwendung von Medizinprodukten. Medizinprodukthersteller müssen nachweisen, dass mögliche Patientenrisiken, die vom Produkt ausgehen, 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 Risiko-Nutzen-Verhältnis bewertet zu werden.
Patientenrisiken können sich beispielsweise durch falsche Ausgaben (z.B. Dosisrechner für Medikamente), fehlende Ausgaben (z. B. Erinnerung für Medikamenteneinnahme) aufgrund von Softwaredefekten (Bugs) oder Sicherheitslücken bei Verwendung auf mobilen Geräten

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 eine App, die ein Medizinprodukt ist, deutlich aufwendiger ist als für eine "normale" App (Verifizierung, Validierung, Dokumentation, Information etc.).

2.9.5 IEC 82304-1:2017 Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit

IEC 82304-1 Health-Software

Die IEC 82304-1 wurde 2016 erstmals veröffentlicht, um bestehende Lücken der IEC 62304 bei der Verwendung für Standalone Software zu schliessen. In den Anwendungsbereich der IEC 82304-1 fallen alle Software-Produkte und Apps, die auf allgemeinen Computersystemen, Handys und Tablets 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.

2.9.6 IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle

IEC 81001-5-1

Die IEC 81001-5-1 ergänzt den in IEC 62304 beschriebenen Software-Lebenszyklus um Prozesse zur Gewährleistung der IT-Sicherheit. Ziel der Norm ist es, die Cybersicherheit von Gesundheits-Software zu erhöhen, indem bestimmte Tätigkeiten und Aufgaben in den Software-Lebenszyklusprozessen festgelegt werden und auch die Sicherheit der Prozesse selbst erhöht wird.

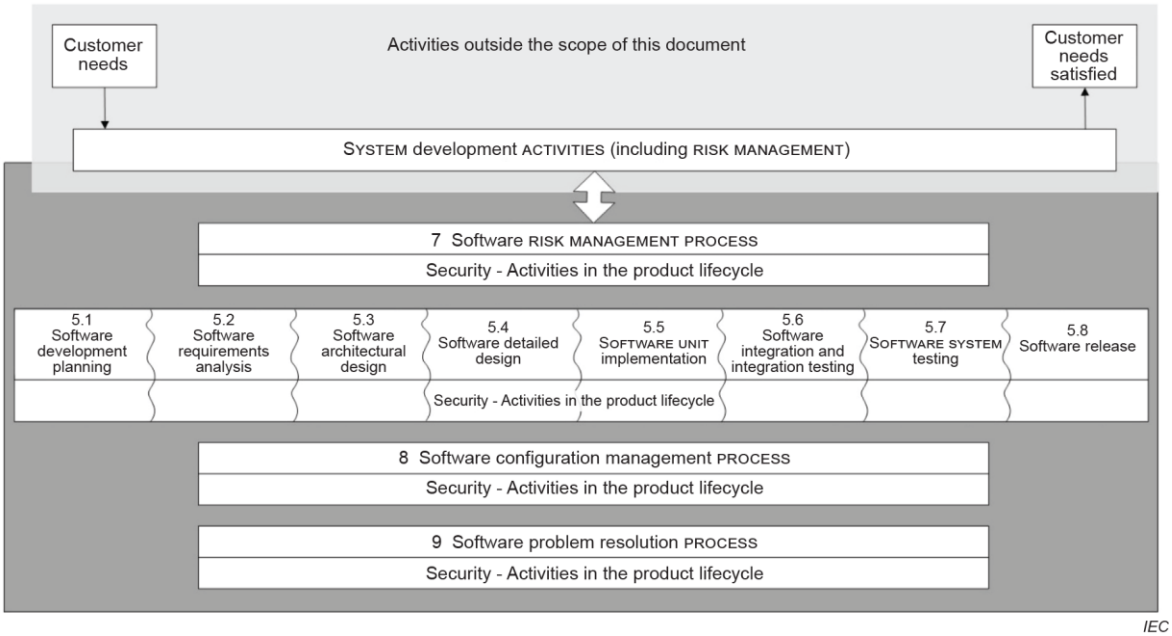

Abbildung 6: IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle (Figure 2)

Die Norm soll für die MDR harmonisiert werden und kann somit zum Nachweis der Erfüllung der grundlegenden Sicherheits- und Leistungsanforderungen herangezogen werden.

2.9.7 IEC TR 60601-4-5:2021 Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications

IEC TR 60601-4-5

Der technische Bericht IEC TR 60601-4-5 beschreibt konkrete Massnahmen, wie IT-Sicherheit bei Medizinprodukten auf technischer Ebene angegangen werden kann. Er bezieht sich dabei auf die für IT-Sicherheit in Industriellen Kommunikationsnetzwerken gedachte IEC 62443-4-2.

Ein Schlüsselelement des IEC TR 60601-4-5sind die Security Levels, welche verwendet werden, um das erforderliche Sicherheitsniveau eines IT-Netzwerks sowie das in einem medizinischen Gerät, respektive in einer Software, implementierte Sicherheitsniveau zu beschreiben. Das Security Level definiert dabei, welche Massnahmen in welchem Umfang implementiert sein müssen. Ziel ist es, dass das erreichte Sicherheitsniveau *(achieved security level SL-A)* nach der Integration der Software in das Netzwerk gleich oder höher ist, wie das zuvor definierte angestrebte Sicherheitsniveau *(target security level SL-T).* Massgeblich dafür ist die Sicherheitsfähigkeit *(capability security level SL-C)* der Software, welche durch die Implementierung der in der Norm beschriebenen technischen Massnahmen definiert wird.

Der technische Bericht bietet Herstellern von medizinischen Apps damit eine Anleitung, die entsprechenden grundlegenden Sicherheits- und Leistungsanforderungen (GSPR) der MDR zu erfüllen.

3 Die Situation Schweiz – EU

3.1 Das Wichtigste in Kürze

Unter den alten Regulierungen (europäische MDD und alte Schweizer MepV) konnten, insbesondere dank dem Mutual Recognition Agreement MRA, Medizinprodukte, die in der Schweiz auf den Markt gebracht wurden, Barrierefrei in Europa vertrieben werden und umgekehrt. Das MRA wurde jedoch nicht für die neuen Regulierungen (europäische MDR und neue Schweizer MepV) aufdatiert. Die gegenseitige Anerkennung ist nicht mehr gegeben und die Schweiz gilt im Sinne der MDR nun als Drittstaat. Als Folge davon müssen Schweizer Hersteller für den Zugang zum EU Markt einen Bevollmächtigten mit Sitz in einem EU-Mitgliedstaat (EU-Rep) benennen und ihre Produkte durch einen EU-Importeur in Verkehr bringen lassen. Da die Swissmedic zudem keinen Zugriff auf die europäische Datenbank für Medizinprodukte EUDAMED hat muss die Registrierung von Wirtschaftsakteuren und Produkten sowie Meldungen über Vorkommnisse direkt an Swissmedic erfolgen.

3.2 Die Schweiz als Drittstaat im Sinne der MDR

Mutual Recognition Agreement MRA

Das Mutual Recognition Agreement MRA zwischen der Schweiz und der EU regelt die gegenseitige Anerkennung von Konformitätsbewertungsverfahren und ist ein wichtiges Instrument zum Abbau technischer Handelshemmnisse bei der Vermarktung zahlreicher Industrieerzeugnisse, unter anderem bei Medizinprodukten. Die gegenseitige Anerkennung der alten europäischen MDD und schweizerischen MepV war Bestandteil des MRA. Diese Verträge vereinfachten Meldepflichten der Inverkehrbringer und erlaubten einen Direktvertrieb von der Schweiz aus in alle EU- und EFTA-Mitgliedstaaten sowie in die Türkei, ohne die Notwendigkeit für einen Bevollmächtigten mit Sitz in diesen Ländern. Umgekehrt konnten Firmen mit Sitz in den Vertragsstaaten konforme Medizinprodukte direkt in der Schweiz vertreiben.

Bis zum Geltungsbeginn der europäischen MDR und dem Inkrafttreten der neuen schweizerischen MepV am 26. Mai 2021 hätte das MRA, um die neuen Verordnungen abzudecken und den freien Marktzugang weiterhin ohne zusätzliche Anforderungen aufrechtzuerhalten, aufdatiert werden müssen.

Die EU hatte im Vorfeld den Abschluss des Institutionellen Rahmenabkommens InstA mit der Schweiz als Bedingung für die Ausarbeitung von weiteren und Aufdatierung von bestehenden Bilateralen Verträgen gestellt. Der Abbruch der Verhandlungen zum InstA seitens des Bundesrats am 26. Mai 2021 führte dazu, dass die EU ih-

rerseits die Überarbeitungen des MRA abgebrochen hat. Die gegenseitige Anerkennung der Medizinprodukteregulierungen zwischen der Schweiz und der EU ist somit nicht mehr gegeben.

Die schweizerische MepV bezieht sich grösstenteils direkt auf die MDR und die Anforderungen an die verschiedenen Wirtschaftsakteure sind in weiten Teilen identisch mit denen der MDR. Prinzipiell liest sich die MepV wie die MDR, wobei gewisse Begriffe angepasst werden (‚EU', ‚Union' oder ‚Mitgliedstaat' wird mit ‚Schweiz' ersetzt, ‚Drittstaat / Drittland' wird als ‚Ausland' oder ‚anderer Staat' bezeichnet). Wenn die MDR also zum Beispiel auf Hersteller aus Drittstaaten Bezug nimmt, was alle nicht-EU/EWR Staaten meint und die Schweiz miteinbezieht, bezeichnet diese die MepV als ‚ausländische Hersteller', was wiederum auch Hersteller aus der EU einschliesst. Durch das überarbeitete MRA hätten Wirtschaftsakteure aus dem europäischen Raum und der Schweiz weitestgehend von den in der MepV und MDR definierten Pflichten für ausländische Wirtschaftsakteure befreit werden sollen.

Dass das MRA nicht für die neuen Regulierungen aufdatiert wurde, hat, insbesondere für Schweizer Hersteller die ihre Produkte in Europa auf den Markt bringen wollen, weitreichende Folgen.

3.3 EU Bevollmächtigter

EU Bevollmächtigter (EU-Rep)

Hersteller aus Drittstaaten, was die Schweiz mit einschliesst, müssen einen Bevollmächtigten (EU-Rep) mit Sitz in einem EU-Mitgliedsstaat benennen, um ihre Produkte in der EU auf den Markt bringen zu können. Der EU-Rep garantiert den EU-Mitgliedsstaaten einerseits eine rechtlich belangbare Entität, andererseits ist er selbst dazu verpflichtet, die Einhaltung der Vorschriften durch den Hersteller zu überprüfen.

Hersteller können jede natürliche oder juristische Person mit Sitz in der EU als ihren EU-Rep benennen. Dazu ist ein schriftliches Mandat nötig, welches von Hersteller und EU-Rep unterzeichnet werden muss. Der EU-Rep muss dauerhaft und ständig auf eine Fachperson zurückgreifen können, welche nachweislich mit den Regulierungsvorschriften für Medizinprodukte in der EU vertraut ist (sog. Person responsible for regulatory compliance PRRC). Weiter muss sich der EU-Rep, wie der Hersteller auch, in EUDAMED (siehe Kapitel 4.3) registrieren und eine Single Registration Number SRN beziehen.

Aufgaben des EU-Rep

Der Bevollmächtigte wird zum primären Ansprechpartner der zuständigen Behörden in der EU und muss folgende Pflichten übernehmen:

- Überprüfung der Einhaltung der Registrierungsvorschriften
  Der Bevollmächtigte hat sicherzustellen, dass der Hersteller eine EU-Konformitätserklärung und eine Technische Dokumentation für seine Produkte erstellt hat. Weiter muss sich der Bevollmächtigte vergewissern, dass ein den Produkten entsprechendes Konformitätsbewertungsverfahren durchgeführt wurde. Der Bevollmächtigte prüft ausserdem, ob sich Hersteller und Importeure korrekt In EUDAMED registriert haben und dass die Produkte eine korrekte UDI-DI erhalten haben und in EUDAMED eingetragen wurden.
- Bereithalten der Dokumentation
  Der EU-Rep muss über Kopien der Technischen Dokumentation, der EU-Konformitätserklärung, sowie allenfalls der Konformitätsbescheinigung der Produkte verfügen. Die Dokumente müssen bis 10 Jahre nach dem letzten Inverkehrbringen der Produkte (15 Jahre bei Implantaten) aufbewahrt werden. Die Dokumente müssen auf Verlangen einer zuständigen Behörde ausgehändigt werden.
- Unterstützung der Behörden bei Audits und Produktprüfungen
  Behörden können den EU-Rep Zugang zu Proben oder Testprodukten ersuchen. Der EU-Rep muss sicherstellen, dass dieser Zugang auch gewährt wird. Weiter unterstützt er die Behörden bei allen Präventiv- oder Korrekturmassnahmen bezüglich fehlerhafter Produkte.
- Meldung von Vorfällen und Beschwerden (Vigilance Report)
  Der EU-Rep muss den Hersteller unverzüglich über Vorkommnisse im Zusammenhang mit Produkten, für welche er verantwortlich ist, unterrichten.

Mithaftung des EU-Rep

Der EU-Rep ist zudem für fehlerhafte Produkte als Gesamtschuldner zusammen mit dem Hersteller haftbar, sofern der Hersteller seinen in der MDR definierten Pflichten nicht nachkommt. Es ist also im eigenen Interesse des EU-Reps die Konformität der Produkte und Einhaltung der Vorschriften durch den Hersteller genau zu überprüfen. Die erweiterte Haftung stellt zudem höhere Anforderungen an den Versicherungsschutz des EU-Reps.

Hersteller sind ihrerseits dazu verpflichtet, ihrem EU-Rep alle benötigten Dokumente lückenlos zur Verfügung zu stellen, was allenfalls

auch vertrauliche Informationen der Technischen Dokumentation der Produkte miteinbezieht.

Kennzeichnung der Produkte

Der EU-Rep muss auf der Kennzeichnung der Produkte angegeben werden (bei Software kann dies, wie auch der Rest der ‚Etikette' z.B. auf einem leicht zugänglichen Infoscreen geschehen). Dazu wird vorzugsweise folgendes Symbol verwendet gefolgt von Name und Anschrift:

Musterfirma
Lietzenburger Strasse 95
DE-84242 Tutzing

Weiter müssen die Informationen zum EU-Rep auch auf der Konformitätserklärung und allenfalls Konformitätsbescheinigung angegeben werden.

EU-Importeur

Neben dem EU-Rep benötigen Hersteller aus Drittstaaten auch einen Importeur, der ihre Produkte im EU Markt in Verkehr bringt. Anders als der EU-Rep werden Importeure jedoch nicht durch den Hersteller benannt – grundsätzlich wird jede natürliche oder juristische Person die ein Produkt aus einem Drittstaat auf dem EU Markt in Verkehr bringt zum Importeur im Sinne der MDR. Dennoch fordert die MDR eine enge Zusammenarbeit zwischen Herstellern und Importeuren, insbesondere bezüglich der Bearbeitung von Beschwerden und Rückrufen.

3.4 Marktüberwachung in der Schweiz

Der Status als Drittstaat hat auch für die Marktüberwachung in der Schweiz grosse Folgen. Mit der MDR wurde die Europäische Datenbank für Medizinprodukte EUDAMED eingeführt (siehe Kapitel 4.3). Sie dient insbesondere dem Informationsaustausch zwischen den zuständigen Behörden der EU Mitgliedsstaaten und soll so die Marktüberwachung und Rückverfolgbarkeit der Produkte erleichtern. In der EUDAMED werden unter anderem Wirtschaftsakteure (Hersteller, Bevollmächtigte, Importeure und allenfalls Händler) und Produkte registriert.

Die MepV wurde weitestgehend and die MDR angepasst und stellt dementsprechend die gleichen Forderungen zur Registrierung von Wirtschaftsakteuren und Produkten. Als Drittstaat hat die Schweiz, respektive die zuständige Behörde Swissmedic, nun aber keinen Zugriff auf die EUDAMED und ein direkter Informationsaustausch

zwischen der Swissmedic und den zuständigen Behörden der EU Mitgliedsstaaten findet nicht statt. Um innerhalb der Schweiz eine funktionierende Marktüberwachung zu gewährleisten müssen sich deshalb Hersteller, Bevollmächtigte und Importeure bei Swissmedic registrieren und eine so genannte Swiss Single Registration Number CHRN, analog zur SRN in Europa, beantragen. Auch Produkte werden in Zukunft über Swissmedic registriert werden müssen. Ab wann dies nötig ist und wie die Produktregistrierung im Detail aussehen wird steht bisher noch nicht fest. Ein der EUDAMED entsprechendes elektronisches System für die Schweiz ist in Arbeit, die genauen Modalitäten sind aber noch nicht bekannt.

Hersteller, die ihre Produkte in der Schweiz und der EU auf den Markt bringen, müssen sich und ihre Produkte also bei der Swissmedic sowie in der EUDAMED registrieren. Auch meldepflichtige Vorkommnisse mit Produkten müssen bei der Swissmedic und, wenn nötig, in der EUDAMED gemeldet werden (siehe Kapitel 4.5).

4 Medizinische Software unter der MepV und MDR

4.1 Das Wichtigste in Kürze

Die Übergangsfrist der neuen Europäischen Medizinprodukteverordnung, kurz MDR, endete am 26.05.2021. Zeitgleich wurde die neue MepV in der Schweiz in Kraft gesetzt. Die MDR und neue MepV brachten einige einschneidende Änderungen mit sich, welche im Besonderen auch von Herstellern von medizinischer Software (Medical Device SW, MDSW) beachtet werden müssen. Dazu gehören eine verschärfte Klassifizierungregel für medizinische Software, erhöhte Anforderungen an klinische Bewertungen, Post-Market Surveillance und Vigilanz, sowie die Einführung der Datenbank für Medizinprodukte EUDAMED.

4.2 Qualifizierung und Klassifizierung

Während die grundsätzliche Definition, die bestimmt, ob eine Software ein Medizinprodukt ist oder nicht, weitestgehend gleich geblieben ist, brachte die MDR folgenschwere Änderungen der Risikoklassifizierung von medizinischer Software mit sich. Ein grosser Teil der Software, welche unter der Medizinprodukterichtlinie MDD als Klasse I eingestuft wurde, ist unter der MDR höher klassifiziert, was einen beträchtlichen Einfluss auf den Aufwand hat, den Hersteller in die Zertifizierung investieren müssen.
Die veränderte Klassifizierung kommt durch Regel 11 aus Anhang VIII (Klassifizierungsregeln) der MDR zustande.

4.2.1 Klassifizierung nach Regel 11

In der MDD wurde medizinische Software gemäss den Klassifizierungsregeln für aktive medizinische Produkte klassifiziert. Diese Regeln sind jedoch nicht spezifisch auf Software ausgelegt, sondern eher auf aktive Geräte, welche dem Körper Energie oder Substanzen zuführen oder diese aus dem Körper entfernen. Auf das Risiko, das durch von einer Software gelieferten Falschinformation für den Patienten entstehen kann, wird dagegen nicht eingegangen.

Verordnung (EU) 2017/745, Anhang VIII

Zu diesem Zweck wurde die Regel 11 in die MDR aufgenommen. Sie besagt, dass:

Klassifizierungsregel 11

Software, die dazu bestimmt ist, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:

- *den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder*
- *eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse IIb zugeordnet.*

Software, die für die Kontrolle von physiologischen Prozessen bestimmt ist, gehört zur Klasse IIa, es sei denn, sie ist für die Kontrolle von vitalen physiologischen Parametern bestimmt, wobei die Art der Änderung dieser Parameter zu einer unmittelbaren Gefahr für den Patienten führen könnte; in diesem Fall wird sie der Klasse IIb zugeordnet.

Sämtliche andere Software wird der Klasse I zugeordnet.

Hinweis: Der Begriff "Kontrolle" wird hier im Sinne von Überwachung (Monitoring) verwendet.

4.2.2 Erläuterung durch die EU – MDCG 2019-11

MDCG 2019-11

Die Medical Device Coordination Group (MDCG) der EU hat im Oktober 2019 einen Leitfaden zur Qualifizierung und Klassifizierung von Medical Device Software (MDSW) unter der MDR und IVDR herausgegeben. Das Dokument ist zwar rechtlich nicht bindend, hat aber grosses Gewicht.

Hilfestellung und Entscheidungsdiagramme

Der Leitfaden liefert eine Hilfestellung bei der Frage nach der Qualifizierung einer Software als Medizinprodukt sowie deren Klassifizierung. Dazu gehört auch eine andere Darstellung der Regel 11, welche aber nicht unbedingt zu einem besseren Verständnis der ohnehin schon klar definierten Regel führt.

Die Regel 11 wird dabei in drei Unterregeln unterteilt, welche abhängig von der Zweckbestimmung der Software zum Tragen kommen:

11a) (Absätze 1 bis 3 von Regel 11) Software, die dazu bestimmt ist, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden (Klasse IIa – III);

11b) (Absatz 4 von Regel 11) Software bestimmt für die Kontrolle von physiologischen Prozessen oder Parametern (Klasse IIa, IIb);

11c) (Absatz 5 von Regel 11) Software bestimmt für alle anderen Zwecke (Klasse I).

Ein Entscheidungsdiagramm und die dazugehörigen Fragen dienen als Hilfestellung bei der Qualifikation einer Software als Medizinprodukt :

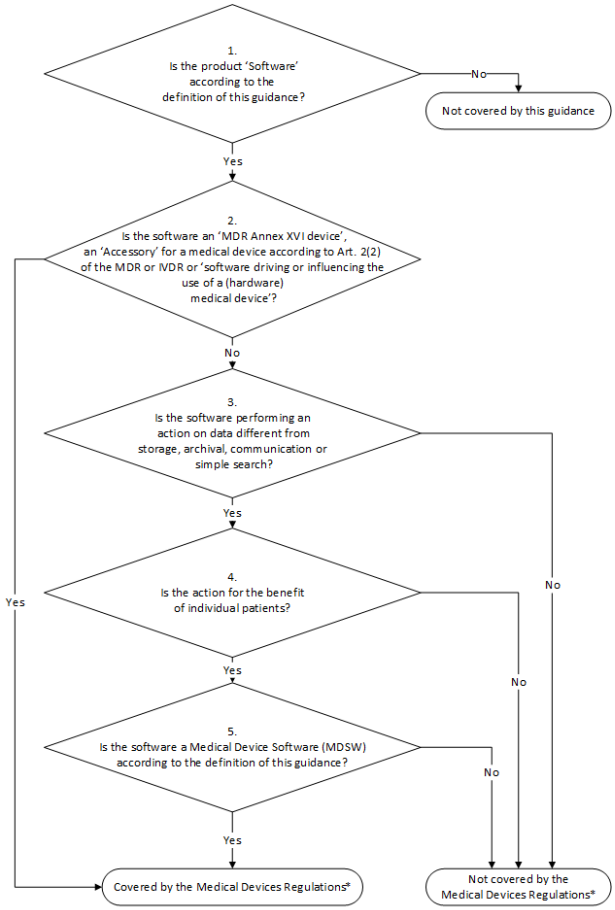

Abbildung 7: Entscheidungsdiagramm für die Qualifikation von Software als Medizinprodukt aus dem MDCG 2019-11 Leitfaden.

Ein weiteres Entscheidungsdiagramm hilft bei der Einschätzung, ob es sich bei der medizinischen Software um ein Medizinprodukt (fällt unter die MDR) oder ein In-vitro-Diagnostikum (fällt unter die IVDR) handelt.

Eine Tabelle veranschaulicht zudem die Zusammenhänge zwischen den IMDRF Risikokategorien (“IMDRF Risk Framework”) und den

MDR Risikoklassen. Dabei werden die Risikoklassen einer Software abhängig von der Kombination aus Bedeutung der von der Software gelieferten Information für eine medizinische Entscheidung und der medizinischen Situation oder dem Zustand des Patienten definiert.

		Significance of Information provided by the MDSW to a healthcare situation related to diagnosis/therapy		
State of Healthcare situation or patient condition		**High** Treat or diagnose *~ IMDRF 5.1.1*	**Medium** Drives clinical management *~ IMDRF 5.1.2*	**Low** Informs clinical management *(everything else)*
	Critical situation or patient condition *~ IMDRF 5.2.1*	**Class III** *Category IV.i*	**Class IIb** *Category III.i*	**Class IIa** *Category II.i*
	Serious situation or patient condition *~ IMDRF 5.2.2*	**Class IIb** *Category III.ii*	**Class IIa** *Category II.ii*	**Class IIa** *Category I.ii*
	Non-serious situation or patient condition *(everything else)*	**Class IIa** *Category II.iii*	**Class IIa** *Category I.iii*	**Class IIa** *Category I.i*

Abbildung 8: Illustration der Zusammenhänge der IMDRF Risikokategorien und der Risikoklassen der MDR (aus dem Leitfaden MDCG 2019-11)

Abschliessend bietet das Dokument noch einige Beispiele, an denen die Regeln zur Qualifikation als Medizinprodukt und zur Klassifizierung veranschaulicht werden.

Das Dokument macht klar, dass die MDCG die Regel 11 eher strikt auslegt. Zum Einen sei das Liefern von Informationen, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, charakteristisch für alle MDSW und somit treffe die Unterregel 11a), welche keine Einteilung zur Klasse I vorsieht, generell auf alle MDSW zu. Zum anderen entsprechen die im IMDRF Dokument definierten Risikokategorien I und II beide der MDR Risikoklasse IIa. Dies verdeutlicht nochmals, dass die meiste medizinische Software unter der MDR nicht mehr der Risikoklasse I zugeteilt werden kann. Als einziges Beispiel für eine solche Klasse I Software nennt das MDCG Dokument eine App, die zur Bestimmung des Fruchtbarkeitszyklus gedacht ist.

4.2.3 Auswirkungen für Hersteller von MDSW

Für Medizinprodukte, die höher klassifiziert sind als Klasse I, müssen die Hersteller bei der Konformitätsbewertung eine Benannte Stelle miteinbeziehen. Das heisst, die Konformität der Software mit den Anforderungen der MDR kann nicht durch den Hersteller selbst in

Eigenverantwortung deklariert werden, sondern muss durch eine Benannte Stelle geprüft und bestätigt werden.
In den meisten Fällen bedeutet dies, dass zusätzlich ein vollständiges Qualitätsmanagementsystem (QMS) nach ISO 13485 aufgebaut und zertifiziert werden muss. Der Aufbau eines QMS bedeutet vor allem für kleinere Firmen und Start-Ups einen massiven zeitlichen und finanziellen Mehraufwand.

Übergangsfrist

Produkte, die unter der MDD als Klasse I galten, und gemäss den Klassifizierungsregeln der MDR hochklassifiziert werden – wie es bei medizinischer Software häufig der Fall ist – dürfen weiterhin bis am 26. Mai 2024 in Verkehr gebracht werden. Voraussetzungen dafür sind, dass die Konformitätserklärung unter MDD vor dem 26. Mai 2021 ausgestellt wurde und dass keine signifikanten Änderungen am Design oder der Zweckbestimmung der Produkte vorgenommen werden. Weiter müssen die Anforderungen der MDR an Post-Market Surveillance und Vigilanz in jedem Fall erfüllt werden.

4.3 Europäische Datenbank für Medizinprodukte EUDAMED

Die MDR hat neu die Datenbank für Medizinprodukte EUDAMED eingeführt. Die Datenbank dient dazu, alle relevanten Informationen zu Wirtschaftsakteuren und Produkten zu zentralisieren und die Rückverfolgbarkeit zu gewährleisten. Die EUDAMED hat insbesondere folgende Ziele:

- Transparenz und angemessener Zugang zu Informationen für Anwender über Produkte und beteiligte Wirtschaftsakteure
- Verbesserung der Marktüberwachung (u. a durch eindeutige Identifizierung von Produkten und erleichterte Rückverfolgbarkeit)
- Vermeidung von Mehrfachberichterstattung
- Verbesserung der Koordination zwischen den Mitgliedstaaten
- Verbesserung des Informationsflusses zwischen Wirtschaftsakteuren, Benannten Stellen (oder Sponsoren) und Mitgliedstaaten und der Kommission

Die EUDAMED besteht aus mehreren Modulen:

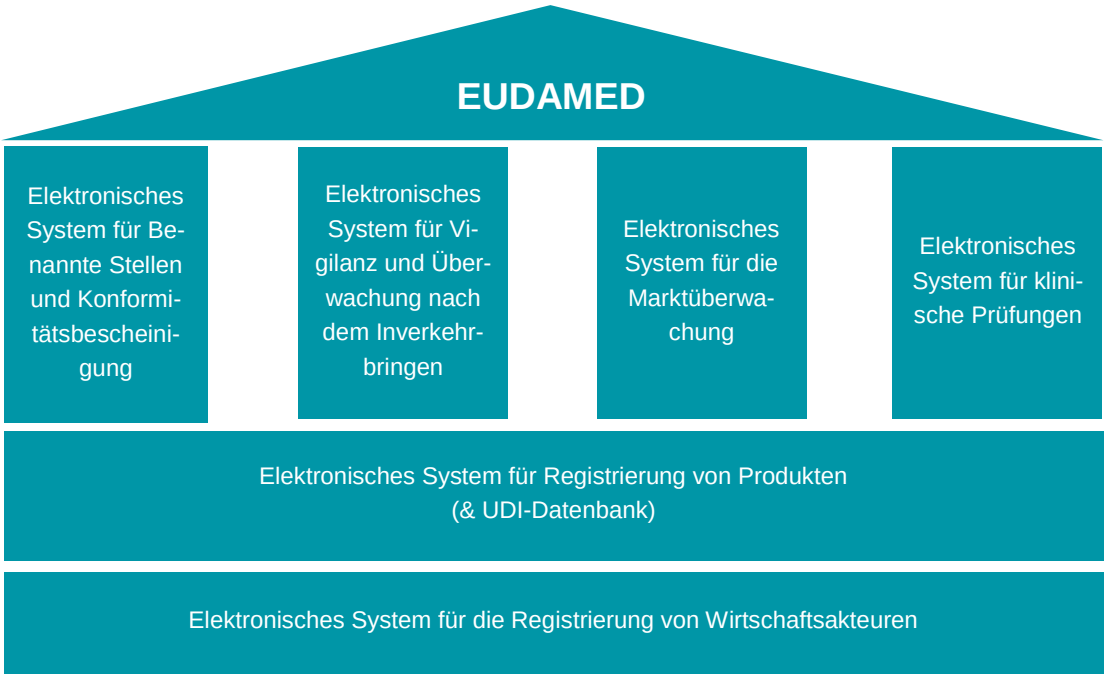

Abbildung 9: Module der EUDAMED (Bild: ISS AG)

Registrierung von Wirtschaftsakteuren

Module der EUDAMED

Hersteller, Importeure und Bevollmächtigte müssen sich in der EUDAMED registrieren. Nach der Registrierung wird dem Wirtschaftsakteur eine Single Registration Number (SRN) zugewiesen, die eine eindeutige Identifizierung erlaubt.

Produktregistrierung/UDI

Dieses Modul wird alle produktspezifischen Informationen in Verbindung mit dem UDI System beinhalten. Das UDI System besteht aus der BASIC UDI-DI, welche alle gemeinsamen Eigenschaften einer Produktgruppe abbildet, und der UDI-DI, die spezifische Produkte identifiziert. Eine BASIC UDI-DI kann demnach mehrere verschiedene UDI-DI beinhalten, wohingegen eine UDI-DI genau einer BASIC UDI-DI zugeordnet wird.

Benannte Stellen und Konformitätsbescheinigungen

In diesem Modul werden Informationen zu den Benannten Stellen und dem Status von Konformitätsbewertungsverfahren verwaltet. Zudem werden von Benannten Stellen ausgestellte Konformitätsbescheinigungen (CE-Zertifikate) gespeichert.

Vigilanz und Produktüberwachung
Hier werden schwerwiegende Vorkommnisse und Sicherheitskorrekturmassnahmen dokumentiert. Weiter werden periodische Sammelmeldungen und Trendmeldungen der Hersteller, sowie Sicherheitsberichte und von den Herstellern übermittelte Sicherheitsanweisungen gespeichert. Dieses System ist direkt mit der UDI Datenbank verknüpft.

Marktüberwachung
Dieses Modul wird in erster Linie von den zuständigen Behörden der Mitgliedstaaten benutzt, um Informationen zur Marktüberwachung auszutauschen.

Klinische Prüfungen
Alle klinischen Prüfungen, die in der EWG durchgeführt werden, müssen ebenfalls in der EUDAMED registriert werden. Klinische Prüfungen können so eindeutig identifiziert und überwacht werden.

Die Daten werden entweder über Online-Formulare eingetragen, oder über eine Schnittstelle (XML) übermittelt.

Dateneintragung und Einführungstermin

Zum heutigen Zeitpunkt sind die Module *Registrierung von Wirtschaftsakteuren*, *Produktregistrierung/UDI* und *Benannte Stellen und Konformitätsbescheinigungen* verfügbar. Die Aufschaltung der restlichen drei Module ist auf Ende 2023 geplant.

Da die Schweiz im Sinne der MDR mittlerweile als Drittstaat gilt (siehe Kapitel 2.9.6) hat die Swissmedic keinen Zugriff auf die EUDAMED. Die MepV stellt jedoch die gleichen Anforderungen bezüglich Registrierungen und Meldungen wie die MDR. Ein entsprechendes System für die Schweiz ist bei der Swissmedic in Bearbeitung. Die Schweizer Medizinprodukte Datenbank wird europäischen EUDAMED ähnlich sein, die genauen Modalitäten sind aber noch nicht bekannt.

Entsprechendes System für die Schweiz

4.4 Klinische Bewertung

Hersteller von Medizinprodukten sind verpflichtet, für all ihre Produkte – unabhängig von der Risikoklassifizierung – eine klinische Bewertung (engl. *clinical evaluation report* CER) zu erstellen. Dabei soll in erster Linie die Sicherheit, die Leistung und der klinische Nutzen von Medizinprodukten demonstriert werden. In der Regel erfor-

dert dieser Nachweis Daten aus der klinischen Anwendung des Medizinproduktes; die Anforderungen an die Menge und Qualität solcher Daten hängen dabei stark von der Risikoklassifizierung ab.

Die klinische Bewertung ist fester Bestandteil des Qualitätsmanagementsystems und der technischen Dokumentation von Medizinprodukten. Sie dient zum Beispiel als Grundlage für das Risikomanagement, indem sie die getroffenen Annahmen zum Nutzen und der Akzeptanz eines Nutzen-Risiko-Verhältnisses begründet.
Eine klinische Bewertung wird zuallererst im Rahmen des Konformitätsbewertungsverfahrens durchgeführt und nach der Markteinführung regelmässig aktualisiert.

4.4.1 Regulatorische Grundlagen und Guidelines

Artikel 61 der MDR definiert die Ziele einer klinischen Bewertung, während Anhang XIV das Vorgehen konkretisiert. Die klinische Bewertung soll basierend auf klinischen Daten demonstrieren, dass ein Produkt die anwendbaren grundlegenden Sicherheits- und Leistungsanforderungen aus Anhang I der MDR erfüllt.

Generell gelten für die klinische Bewertung von medizinischer Software die gleichen Anforderungen wie für alle anderen Medizinprodukte. Das International Medical Device Regulators Forum IMDRF hat zudem eine Guideline (IMDRF/SaMD WG/N41) herausgegeben, welche auf die Eigenheiten der klinischen Bewertung von Software eingeht. Weiter hat die MDCG im März 2020 die Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software - MDCG 2020-1 veröffentlicht, die sich auch auf das IMDRF Dokument bezieht.

4.4.2 Klinische Daten

Klinische Daten

Die klinische Bewertung ist ein systematischer und geplanter Prozess zur kontinuierlichen Generierung, Sammlung, Analyse und Bewertung der klinischen Daten zu einem Produkt.

Klinische Daten bezeichnen Angaben zur Sicherheit oder Leistung, die im Rahmen der klinischen Anwendung eines Produkts gewonnen werden und die aus den folgenden Quellen stammen:

- klinische Prüfungen des betreffenden Produkts,
- klinische Prüfungen oder sonstige in der wissenschaftlichen Fachliteratur wiedergegebene Studien über ein Produkt, dessen

Gleichartigkeit mit dem betreffenden Produkt nachgewiesen werden kann,

- in nach dem Peer-Review-Verfahren überprüfter wissenschaftlicher Fachliteratur veröffentlichte Berichte über sonstige klinische Erfahrungen entweder mit dem betreffenden Produkt oder einem Produkt, dessen Gleichartigkeit mit dem betreffenden Produkt nachgewiesen werden kann,
- klinisch relevante Angaben aus der Überwachung nach dem Inverkehrbringen, insbesondere aus der klinischen Nachbeobachtung nach dem Inverkehrbringen.

Klinische Daten können also über verschiedene Wege gesammelt werden: entweder durch klinische Studien mit dem betreffenden oder einem gleichartigen Produkt, durch Daten aus Fachliteratur zu gleichartigen Produkten, aus Informationen aus Datenbanken zu Produktsicherheit oder durch die Produktüberwachung nach dem Inverkehrbringen (PMS, Vigilance). Für Produkte der Klasse III und implantierbare Produkte ist eine klinische Studie mit dem betreffenden Produkt in den meisten Fällen zwingend. Alle tiefer klassifizierten Produkte können für die klinische Bewertung auch auf Daten zurückgreifen, welche durch klinische Erfahrungen mit gleichartigen Produkten gewonnen wurden.

Damit ein Produkt als gleichartig gilt, muss es bestimmte Eigenschaften mit dem eigenen Produkt teilen. Im Falle von Software sind dies technische Aspekte wie ähnliche Anwendungsbedingungen, Spezifikationen und Eigenschaften (Software Algorithmen) und ähnliche Entwicklungsmethoden, Funktionsgrundsätze und Leistungsanforderungen. Zudem müssen Produkte unter gleichen klinischen Bedingungen und zum gleichen klinischen Zweck angewendet werden, sie müssen also zum Beispiel die gleiche Krankheit und ähnliche Patientenpopulationen behandeln sowie die gleichen Anwender haben und auch ähnliche entscheidende Leistungen bringen.

4.4.3 Klinische Bewertung von Software

Anforderungen an Klinische Bewertung

Standalone Software unterscheidet sich von klassischen Medizinprodukten in einigen Punkten, die sich auch auf die klinische Bewertung auswirken.

Die IMDRF Guideline Software as a Medical Device (SaMD): Clinical Evaluation IMDRF/SaMD WG/N41 definiert die klinische Beurteilung

von medizinischer Software als die Bewertung und Analyse von klinischen Daten, um die klinische Sicherheit, Leistung und Wirksamkeit des Geräts bei bestimmungsgemässer Verwendung zu überprüfen. Sie basiert auf den folgenden drei Prinzipien:

- Valider klinischer Zusammenhang: Gibt es einen validen klinischen Zusammenhang zwischen dem Output der Software und dem klinischen Zustand, auf den die Software abzielt?
- Analytische/Technische Validierung: Verarbeitet die Software die Eingabedaten korrekt, um genaue, zuverlässige und präzise Ausgabedaten zu erzeugen?
- Klinische Validierung: Erreicht die Verwendung der genauen, zuverlässigen und präzisen Ausgabedaten der Software den beabsichtigten Zweck in der Zielpopulation im Kontext der klinischen Versorgung?

Ein valider klinischer Zusammenhang kann prinzipiell über die Studie von klinischer Literatur nachgewiesen werden. Hier gilt es zu zeigen, dass die Daten, welche die Software liefert, also z. B. ein Konzept, eine Schlussfolgerung, oder eine Messung, auch tatsächlich klinisch akzeptiert oder fundiert sind und einen Bezug zur Krankheit oder dem klinischen Zustand hat, auf die die Software abzielt.

Die analytische/technische Validierung soll bestätigen, dass die Software korrekt konstruiert wurde - d.h., dass sie Eingabedaten korrekt und zuverlässig verarbeitet und Ausgabedaten mit dem entsprechenden Grad an Genauigkeit sowie Wiederholbarkeit und Reproduzierbarkeit (d. h. Präzision) erzeugt. Weiter zeigt sie, dass die Software ihre Spezifikationen erfüllt und dass diese Softwarespezifikationen den Benutzeranforderungen und dem Verwendungszweck entsprechen. Diese Informationen werden normalerweise während der Verifizierungs- und Validierungs-Phase des Software-Entwicklungslebenszyklus generiert.

Die klinische Validierung misst schliesslich die Fähigkeit einer Software, für die entsprechende Gesundheitssituation klinisch relevante Ergebnisse zu liefern. Klinisch relevant sind in diesem Zusammenhang positive Auswirkungen einer Software auf die Gesundheit einer Einzelperson oder der Bevölkerung, welche als messbare, patientenrelevante klinische Ergebnisse insbesondere in Zusammenhang mit den Funktionen der Software (also z. B. Diagnose, Behandlung, Risikovorhersage, Vorhersage des Ansprechens auf eine Behandlung) definiert sind. Die klinische Validierung einer Software kann

auch als die Beziehung zwischen den Ergebnissen der Verifizierung und Validierung des Software-Algorithmus und den betreffenden klinischen Zuständen betrachtet werden.
Eine medizinische Software kann laut dem IMDRF Dokument auf verschiedene Arten klinisch validiert werden:

- Durch Bezugnahme auf vorhandene Daten aus Studien, die für den gleichen Verwendungszweck durchgeführt wurden;
- Durch Bezugnahme auf vorhandene Daten aus Studien, die für einen anderen Verwendungszweck durchgeführt wurden, wenn eine Extrapolation solcher Daten gerechtfertigt werden kann; oder
- Durch Generierung neuer klinischer Daten für einen bestimmten Verwendungszweck.

Hier ist anzumerken, dass es durch die verschärften Anforderungen der MDR an die Gleichartigkeit von Produkten schwierig werden wird, die klinische Validierung basierend auf Daten aus Studien mit anderen Produkten durchzuführen.

4.5 Post-Market Surveillance und Vigilanz

PMS und Vigilanz

Die MDR legt einen besonderen Schwerpunkt auf die Erfassung klinischer und sicherheitsrelevanter Daten (im Englischen *Post-Market Surveillance*, kurz PMS genannt) nach der CE-Zertifizierung (Selbstdeklaration für Klasse I) und dem Marktzugang. Die Überwachung der Produktleistung von CE-gekennzeichneten Produkten ist entscheidend, um Risiken in der praktischen Anwendung (und somit auch bisher unbekannte Risiken) des Produkts systematisch zu identifizieren und den Nutzen des Medizinprodukts kontinuierlich zu belegen. Nur durch eine kontinuierliche und systematische Überwachung können Hersteller sicherstellen, dass ihre Medizinprodukte sicher sind und keine unkontrollierten Risiken bestehen.

4.5.1 Regulatorische Grundlagen

PMS-Anforderungen

Artikel 83 der MDR definiert die Überwachung nach dem Inverkehrbringen als einen proaktiven und systematischen Prozess, den die Hersteller umsetzen und (zusammen mit anderen Wirtschaftsbeteiligten) durchführen, um aus Informationen über die Verwendung der Medizinprodukte sowie deren Leistung Präventiv- oder Korrekturmassnahmen (CAPA) abzuleiten.

Auch die Anforderungen an die Überwachung nach dem Inverkehrbringen richten sich nach einem risikobasierter Ansatz, denn das System zur Überwachung nach dem Inverkehrbringen muss der Risikoklasse und der Art des Produktes angemessen sein. Für alle Medizinprodukte, unabhängig von ihrer Risikoklasse, sind Überwachungsaktivitäten erforderlich, diese unterscheiden sich aber in der Art der Anforderungen.

Die Auswertung von gesammelten Daten kann dazu führen, dass die technische Dokumentation aktualisiert wird, denn die Daten aus der Überwachung nach dem Inverkehrbringen dienen dem Zweck,

- die Nutzen-Risiko-Abwägung zu aktualisieren;
- das Risikomanagement zu verbessern;
- die Informationen zur Herstellung, der Gebrauchsanweisung; und der Kennzeichnung zu aktualisieren;
- die klinische Bewertung zu aktualisieren (s. Kapitel 4.4);
- den Kurzbericht über Sicherheit und klinische Leistung zu aktualisieren (nur für Klasse III oder implantierbare Produkte anwendbar);
- den Bedarf an Präventiv-, Korrektur- oder Sicherheitskorrekturmassnahmen im Feld zu ermitteln;
- Trends zu erkennen.

Die Hersteller müssen ihr Post-Market-Überwachungssystem auf einen Überwachungsplan stützen (Artikel 84), der zudem Teil der technischen Dokumentation ist und dazu dient, die Einhaltung der PMS-Anforderungen gemäss den Vorgaben der MDR nachzuweisen. Anhang III spezifiziert die Anforderungen und den Inhalt eines solchen Überwachungsplans, der sich mit der Erfassung und Nutzung der Post-Market-Informationen befasst und mindestens Folgendes umfassen muss:

- ein proaktives und systematisches Verfahren zur Erfassung relevanter verfügbarer Informationen. Das Verfahren ermöglicht

eine ordnungsgemässe Charakterisierung der Leistung der Produkte sowie einen Vergleich zwischen dem Produkt und ähnlichen Produkten auf dem Markt,

- wirksame und geeignete Methoden und Prozesse zur Bewertung der erhobenen Daten,
- geeignete Indikatoren und Schwellenwerte, die im Rahmen der kontinuierlichen Neubewertung der Nutzen-Risiko-Analyse und des Risikomanagements verwendet werden,
- wirksame und geeignete Methoden und Instrumente zur Prüfung von Beschwerden und Analyse von marktbezogenen Erfahrungen, die im Feld erhoben wurden,
- Methoden und Protokolle zur Behandlung der Ereignisse, die der Trendmeldung gemäss Artikel 88 unterliegen, einschliesslich der Methoden und Protokolle, die zur Feststellung jedes statistisch signifikanten Anstiegs der Häufigkeit oder des Schweregrades dieser Vorkommnisse anzuwenden sind, sowie den Beobachtungszeitraum;
- Methoden und Protokolle zur wirksamen Kommunikation mit zuständigen Behörden, Benannten Stellen, Wirtschaftsakteuren und Anwendern;
- Bezugnahme auf Verfahren zur Erfüllung der Verpflichtungen der Hersteller im Zusammenhang mit der Überwachung nach dem Inverkehrbringen;
- systematische Verfahren zur Ermittlung und Einleitung geeigneter Massnahmen, einschliesslich Korrekturmassnahmen;
- wirksame Instrumente zur Ermittlung und Identifizierung von Produkten, die gegebenenfalls Korrekturmassnahmen erfordern, und
- einen Plan für die klinische Nachbeobachtung nach dem Inverkehrbringen gemäss Anhang XIV Teil B oder eine Begründung, warum eine klinische Nachbeobachtung nach dem Inverkehrbringen nicht anwendbar ist.

Die MDR spezifiziert in Anhang III welche Daten als verfügbare Informationen in die Überwachung fliessen und somit proaktiv und systematisch erhoben und verwendet werden müssen:

- Informationen über schwerwiegende Vorkommnisse, einschliesslich Informationen aus den Sicherheitsberichten, und Sicherheitskorrekturmassnahmen im Feld,
- Aufzeichnungen über nicht schwerwiegende Vorkommnisse und Daten zu etwaigen unerwünschten Nebenwirkungen,
- Informationen über die Meldung von Trends,
- einschlägige Fachliteratur oder technische Literatur, Datenbanken und/oder Register,
- von Anwendern, Händlern und Importeuren übermittelte Informationen, einschliesslich Rückmeldungen und Beschwerden,
- öffentlich zugängliche Informationen über ähnliche Medizinprodukte.

4.5.2 Bericht über die Überwachung nach dem Inverkehrbringen

Überwachungsbericht

Die Hersteller von Medizinprodukten aller Klassen sind verpflichtet, einen Bericht über die Überwachung nach dem Inverkehrbringen *(*engl. *post-market surveillance report)* zu erstellen, um die Ergebnisse und Schlussfolgerungen der gesammelten Daten gemäss der Definition im PMS-Plan zusammenzufassen (Artikel 85). Der Bericht muss zudem eine Begründung und Beschreibung der getroffenen Präventiv- und Korrekturmassnahmen enthalten, welche bei Bedarf aktualisiert werden müssen.

4.5.3 Regelmässig aktualisierter Bericht über die Sicherheit

Sicherheitsbericht (PSUR)

Weitere Anforderungen zu erfüllen haben Hersteller von Medizinprodukten der Klassen IIa, IIb und III, diese müssen während der gesamten Lebensdauer des betreffenden Produkts zusätzlich einen Sicherheitsbericht (engl. *peridoic safety update report* - PSUR) erstellen und diesen regelmässig aktualisieren (Artikel 86). Dieser Bericht enthält die Ergebnisse und Schlussfolgerungen der PMS-Daten in Bezug auf die Nutzen-Risiko-Abwägung, Beschrieb und

Erläuterung der vorgenommenen Präventiv- und Korrekturmassnahmen, die wichtigsten Ergebnisse des Bewertungsberichts, die Gesamtabsatzmenge des Produkts sowie Informationen zu Personen, bei denen das Produkt zur Anwendung kommt.

Der Sicherheitsbericht ist Teil der technischen Dokumentation und muss mindestens alle zwei Jahre für Produkte der Klasse IIa und jährlich für Produkte der Klasse IIb und III aktualisiert werden. Die Hersteller müssen Sicherheitsberichte von Produkten der Klassen IIa und IIb ihren Benannten Stellen, und auf Anfrage den zuständigen Behörden, zur Verfügung stellen.

Der Sicherheitsbericht von Produkten der Klasse III ist zudem der Benannten Stelle (via EUDAMED, sobald die Datenbank eingeführt ist) vorzulegen. Die Benannte Stelle fügt ihre Bewertung dem Bericht hinzu und die beiden Dokumente werden anschliessend (wieder via EUDAMED) den zuständigen Behörden zur Verfügung gestellt. Ein periodischer Sicherheitsbericht kann mehrere Medizinprodukte beinhalten. Zurzeit befindet sich eine PSUR Guidance wie auch ein Template auf europäischer Ebene in Arbeit.

4.5.4 Anforderungen betreffend klinischer Nachbeobachtung nach dem Inverkehrbringen (PMCF)

PMCF

Anhang XIV Teil B verlangt das alle Hersteller im Rahmen der klinischen Nachbeobachtung nach dem Inverkehrbringen (engl. *Post-Market Clinical Follow-up* – PMCF) eines Produkts systematisch klinische Daten sammeln, um wichtige Fragen zur Sicherheit und Leistungsfähigkeit des Medizinproduktes zu beantworten und die klinische Bewertung zu aktualisieren.

Daten und Informationen aus der Überwachung nach dem Inverkehrbringen müssen in den Post-Market-Abschnitt der klinischen Bewertung (CER) aufgenommen werden.

Hersteller müssen ihren PMCF-Prozess auf einen Plan stützen und die Ergebnisse der klinischen Nachbeobachtung im Markt in einem Bewertungsbericht dokumentieren, welcher Teil des klinischen Bewertungsberichts und der technischen Dokumentation ist. Die

Schlussfolgerungen des PMCF können auch zu einer Aktualisierung der Risikomanagement-Dokumente führen.

4.5.5 Vigilanz

Vigilanz

Die Vigilanz ist Teil der Überwachung nach dem Inverkehrbringen und bezeichnet das reaktive Meldesystem. Es regelt, in welchem Rahmen Hersteller Vorkommnisse den Behörden melden, sowie die Vorgaben für Sicherheitskorrekturmassnahmen im Feld (FSCAs) und Rückrufe. Artikel 87 der MDR definiert die Vorfälle, welche Hersteller an die zuständigen Behörden melden müssen, wie diese Berichte einzureichen sind und verpflichtet die Hersteller, ihre Vigilanz-Daten zu analysieren.

Hersteller sind verpflichtet jedes schwerwiegende Vorkommnis im Zusammenhang mit ihrem Produkt sowie jede Sicherheitskorrekturmassnahme im Feld unverzüglich zu melden. Für die Meldung von Vorkommnissen muss seit Januar 2020 das Manufacturer Incident Report-Formular (MIR-Formular) genutzt werden. Die MDR stellt spezifische Anforderungen an die Vigilanz und definiert die folgenden Meldefristen für die unterschiedlichen Ereignisse:

- Schwerwiegendes Vorkommnis: unverzüglich, nicht später als nach 15 Tagen
- Schwerwiegende Gefahr für die öffentliche Gesundheit: unverzüglich, nicht später als nach 2 Tagen
- Tod oder unvorhergesehene schwerwiegende Verschlechterung des Gesundheitszustands: unverzüglich, nicht später als nach 10 Tagen

Zudem müssen alle schwerwiegenden Vorkommnisse vom Hersteller untersucht werden, dazu gehört auch eine Risikobewertung der Vorkommnisse und der Sicherheitskorrekturmassnahmen im Feld. Der Hersteller sorgt dafür, dass die Informationen über die ergriffenen Sicherheitskorrekturmassnahmen im Feld den Anwendern des betreffenden Produkts unverzüglich mitgeteilt werden (via EUDAMED, sobald die Datenbank eingeführt ist).

Die MDR erlaubt Herstellern in Absprache mit den zuständigen Behörden periodische Sammelmeldungen von ähnlichen schwerwie-

genden Vorkommnissen im Zusammenhang mit demselben Produkt/derselben Produktart mitzuteilen. Dafür muss die Ursache für die Vorkommnisse bereits festgestellt und gut dokumentiert sein (möglicherweise wurde auch bereits eine Sicherheitskorrekturmassnahme im Feld ergriffen). Die Behörden und Hersteller müssen sich zudem über Form, Inhalt und Häufigkeit dieser periodischen Sammelmeldungen einigen.

Artikel 88 der MDR regelt zudem die Meldung von Trends, da Hersteller verpflichtet sind, statistisch signifikante Anstiege der Häufigkeit oder des Schweregrads nicht schwerwiegender Vorkommnisse oder erwarteter unerwünschter Nebenwirkungen zu überwachen und zu melden. Solche Trends haben eine Auswirkung auf die Nutzen-Risiko-Analyse und müssen auf nicht akzeptable Risiken untersucht werden. Im Rahmen des Plans zur Überwachung nach dem Inverkehrbringen legt der Hersteller den Beobachtungszeitraum fest, sowie welche Methodik angewendet wird, um den statistisch signifikanten Anstieg der Häufigkeit oder des Schweregrads dieser Vorkommnisse festzustellen.

5 MedTech und agile Entwicklung, geht das?

5.1 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.

5.2 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:

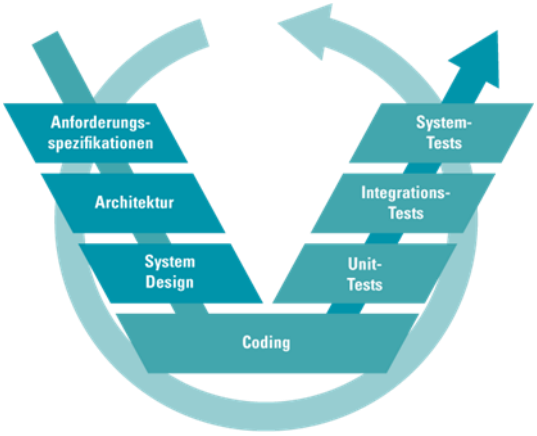

Abbildung 10: vereinfachtes V-Modell (Bild: ISS AG)

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.

5.3 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.

5.3.1 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.

6 Cybersecurity (Datensicherheit)

6.1 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

Aufgrund des von der MDR und MepV 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. Insbesondere medizinische Software wird durch die neue Klassifizierungsregel 11 meist in eine der höheren Risikoklassen eingestuft. Höhere Risikoklassen bedeuten höhere regulatorische Anforderungen, die auch die Sicherheit und den Nachweis der Sicherheit betreffen. Bei der Zertifizierung von Software im oder als Medizinprodukt muss dokumentiert und nachgewiesen werden, dass 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 (siehe Kapitel 2.9.4) 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 (siehe Kapitel 2.9.2) sowie IEC 82304 (siehe 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 Verordnungen impliziert, da ein angemessenes Sicherheitskonzept verlangt wird. Sobald eine Benannte Stelle involviert ist, wird dieser beurteilen, ob die vorgenommenen Massnahmen angemessen und ausreichend sind. Die MDR referenziert zudem die Norm IEC 62304, die das Thema Cybersecurity nur streift, aber doch explizit aufgreift

Weiter werden die Normen IEC 81001-5-1 und IEC TR 606061-4-5 für die MDR harmonisiert. Beide Normen adressieren die Cybersicherheit von Medizinprodukten in Netzwerken (siehe Kapitel 2.9.6 und 2.9.7).

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. Im Juli 2019 hat die Therapeutic Goods Administration in Australien die Medical device cyber security guidance for industry herausgegeben, welche sich mit Cybersecurity und Datenschutz beschäftigt.
Im Januar 2020 hat die MDCG eine Leitlinie zu Cybersecurity für den Rechtsrahmen der MDR und der IVDR herausgegeben. MDCG 2019-16 soll Hersteller dabei unterstützen die Anforderungen des

Anhangs I der MDR an die Cybersecurity zu erfüllen. Das Dokument erläutert unter anderem welche Anforderungen der EU-Verordnungen einen Bezug zur Cybersecurity haben und verweist auf weitere regulatorisch relevante Dokumente (wie z.B. die IMDRF-Guidance).

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 Interface 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:

Schutzobjekte

In einem ersten Schritt werden die zu schützenden Objekte oder Prozesse aufgelistet. **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

Potentielle Angreifer werden identifiziert sowie deren Motivation und die jeweilige Wahrscheinlichkeit eines Angriffs definiert.

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

Angriffsvektoren

Zuletzt werden mögliche Angriffsvektoren, d.h. Wege und Mittel, mit denen ein Angreifer Zugriff auf ein System erhalten könnte, beschrieben.

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

Sicherheitskonzepte

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

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

Diese Konzepte dienen auch als Grundlage zur Gewährleistung der Datensicherheit im Zusammenhang mit dem Datenschutz und entsprechenden Vorgaben aus dem Datenschutzgesetz.

7 Rechtsgrundlage Datenschutz und -sicherheit in der Schweiz

7.1 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.

7.2 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.

7.3 Notwendigkeit zur Beachtung der EU-Datenschutzgesetzgebung

Datenschutz auf EU-Ebene

Im Weiteren ist darauf hinzuweisen, dass seit dem 25. Mai 2018 die neue EU-Datenschutzgesetzgebung in Kraft ist. 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.

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.

Analyse im Einzelfall immer nötig

8 DiGA – Digitale Gesundheitsanwendungen

8.1 Das Wichtigste in Kürze

In Deutschland wurde mit dem Digitale-Versorgung-Gesetz (DVG) die ‚App auf Rezept' eingeführt. Digitale Gesundheitsanwendungen (DiGA) sind Apps, Desktop- oder Browseranwendungen, welche von Ärzten und Psychotherapeuten verordnet und durch die Krankenkasse erstattet werden. Um in das DiGA Verzeichnis der erstattungsfähigen Apps aufgenommen zu werden, muss ein Fast-Track-Prüfverfahren beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) durchlaufen werden. Die Anforderungen an DiGAs sind dabei umfangreich und gehen über jene an medizinische Software hinaus. Unter anderem müssen hohe Anforderungen an Datenschutz, Informationssicherheit und Interoperabilität erfüllt werden. Desweitern müssen für eine dauerhafte Aufnahme im DiGA Verzeichnis positive Versorgungseffekte der DiGA mittels einer vergleichenden Studie nachgewiesen werden.

8.2 Was sind DiGA

Europaweit existieren verschiedene Ansätze und Umsetzungen um die Digitalisierung im Gesundheitswesen weiter voranzutreiben. Die EU Kommission arbeitet zum Beispiel an einem Rechtsrahmen für die digitale Transformation in allen EU-Mitgliedstaaten, welcher auch Vorschriften für Medizinprodukte enthält. Auf nationaler Ebene sind verschiedene Projekte umgesetzt worden, unter anderem bei elektronischen Patientenakten und Verschreibungen.

App auf Rezept

Deutschland hat mit dem Digitale-Versorgung-Gesetz (DVG) die ‚App auf Rezept' eingeführt. Die sogenannten digitalen Gesundheitsanwendungen (DiGA), wobei es sich um Apps auf einem Smartphone aber auch Desktop- oder Browseranwendungen handeln kann, werden von Ärzten und Psychotherapeuten verordnet und durch die Krankenkasse erstattet. Voraussetzung dafür ist das erfolgreiche Durchlaufen eines Prüfverfahrens beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) und Aufnahme in das DiGA-Verzeichnis.

Voraussetzungen

Um in das DiGA-Verzeichnis aufgenommen zu werden, müssen die Apps gewisse Eigenschaften aufweisen. Zurzeit sind nur Medizinprodukte der Klasse I und IIa nach MDR (resp. MDD während der Übergangszeit) zugelassen. Angesichts der tendenziell höheren Klassifizierung von Software unter der MDR wird diese Einschränkung womöglich in Zukunft aufgehoben. Der medizinische Zweck

der App muss primär durch die digitale Hauptfunktion erreicht werden. Software, welche ausschliesslich ein anderes Medizinprodukt steuert oder ausliest gehört demnach nicht dazu. Eine DiGA unterstützt die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen. Apps, welche zur Primärprävention gedacht sind (Verhinderung von Erkrankungen von nicht kranken Menschen) sind ausgeschlossen. Funktionen für die Sekundär- (Verhindern der Verschlechterung eines Krankheitszustandes) und Tertiärprävention (Vermeiden von Folgeerkrankungen oder Komplikationen) fallen hingegen unter ‚Behandlung' und können Bestandteil einer DiGA sein. Weiter müssen DiGA immer vom Patienten (alleine oder zusammen mit den Leistungserbringenden) eingesetzt werden, und nicht nur durch den Arzt für die Behandlung von Patienten. Eine DiGA kann auch zusammen mit Hardware betrieben werden, wenn zum Beispiel Daten von einer Smartwatch bezogen werden.

8.3 Das DiGA Verzeichnis

DiGA Verzeichnis des BfArM

Im DiGA Verzeichnis werden alle DiGAs aufgelistet die das Prüfverfahren erfolgreich absolviert haben und durch die Krankenkasse erstattet werden. Das Verzeichnis bietet transparente und umfassende Informationen bezüglich Leistungsfähigkeit und Eigenschaften der DiGAs für Patienten und Leistungserbringer, soll aber auch die Integration von DiGAs in die Strukturen und Prozesse der Gesundheitsversorgung auf technischer, organisatorischer und praktischer Ebene erleichtern.

Das Verzeichnis beinhaltet Basisdaten zum Medizinprodukt (Produktbezeichnung, involvierte Benannte Stelle, Zweckbestimmung und Gebrauchsanweisung, Haftpflichtversicherung des Herstellers inkl. Deckungssumme, etc.), Informationen für Versicherte und Patienten (Zielsetzung, Wirkungsweise, Inhalt, Funktionen und Nutzung der DiGA, Checklisten zu Datenschutz und Qualitätsanforderungen, Standort der Datenverarbeitung und anfallende Mehrkosten für optionales Zubehör), Informationen für Leistungserbringende (Patientengruppe/Indikation, positive Versorgungseffekte, Einordnung in den Versorgungspfad, empfohlene Nutzungsdauer, Erläuterung der vorgesehenen Nutzerrollen, etc.), medizinische Fachinformationen (Studienbericht zum Nachweis positiver Versorgungseffekte, beteiligte medizinische Einrichtungen und Organisationen, etc.) sowie

technische Informationen (Kompatibilitätszusagen in Bezug auf unterstützte Plattformen und Geräte, für den Datenaustausch genutzte Standards und Profile).

Vorläufige und dauerhafte Aufnahme

Hersteller können für ihre Anwendungen entweder eine vorläufige oder dauerhafte Eintragung in das DiGA Verzeichnis beantragen. Um dauerhaft im DiGA Verzeichnis aufgenommen zu werden, muss eine vergleichende Studie zum Nachweis eines positiven Versorgungseffektes vorgewiesen werden.
Falls noch keine solche Studie erfolgreich durchgeführt wurde, die Anforderungen ansonsten aber erfüllt sind, können Hersteller eine vorläufige Aufnahme beantragen. Die DiGA wird dabei in das Verzeichnis aufgenommen und ist auch bereits vollumfänglich erstattungsfähig. Nach 12 Monaten muss der Hersteller die vergleichende Studie zum Nachweis positiver Versorgungseffekte abgeschlossen haben, in Einzelfällen kann die Erprobungszeit um weitere 12 Monate verlängert werden. Das BfArM Prüft die Ergebnisse und entscheidet über die dauerhafte Aufnahme der DiGA innerhalb von 3 Monaten. Bei einem negativen Entscheid wird die DiGA aus dem Verzeichnis gestrichen und der Hersteller kann erst nach 12 Monaten und nur mit einer erfolgreich abgeschlossenen Studie einen erneuten Antrag zur dauerhaften Aufnahme stellen (eine zweite vorläufige Aufnahme ist nicht mehr möglich).

Antragsverfahren

Das Antragsverfahren für DiGAs erfolgt über das Antragsportal des BfArM. Sobald alle Pflichtangaben und dazugehörigen Dokumente online überstellt wurden, prüft das BfArM die formale Vollständigkeit. Sind alle Angaben vollständig, teilt das BfArM dies innert 14 Tagen mit und bestätigt das Eingangsdatum als Beginn der Bearbeitungsfrist. Bei unvollständigen Unterlagen hat der Antragsteller bis zu drei Monate Zeit um den Antrag entsprechend zu ergänzen. Mit Eingang der vollständigen Unterlagen beginnt die maximal 3 monatige Bewertungszeit. Während der Prüfung kann das BfArM weitere Unterlagen oder Klärungen beantragen, wobei für die Beantwortung eine Frist gesetzt wird. Dabei wird die 3 monatige Bewertungszeit aber nicht verlängert, das heisst alle Nachforderungen müssen innerhalb dieser Frist erledigt sein.

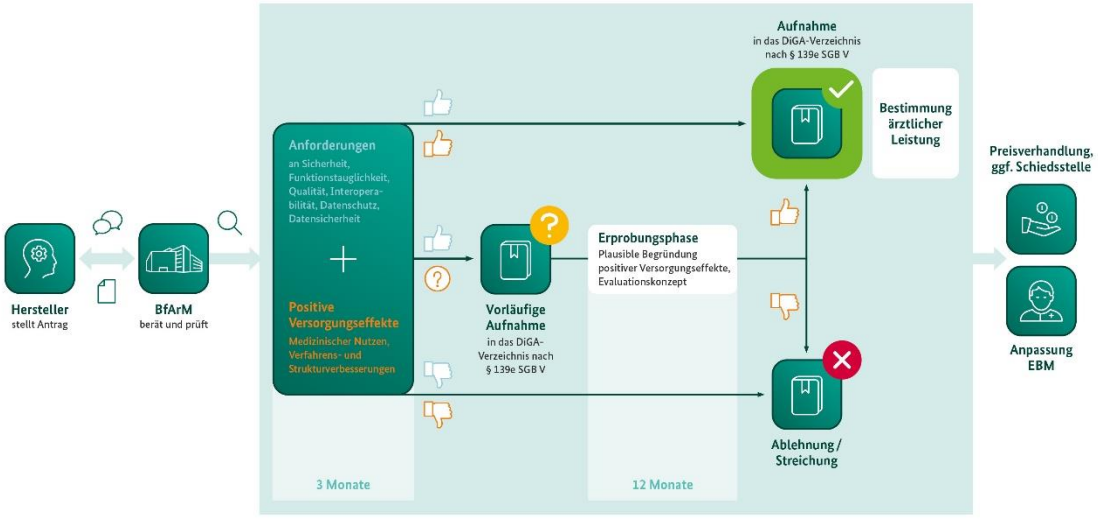

Abbildung 11: Ablauf des DiGA Fasttrack-Verfahrens. Quelle: BfArM

8.4 Anforderungen an DiGA und Hersteller

Die Anforderungen an eine DiGA sind in den Paragraphen 3 bis 6 der DiGA-Verordnung (DiGAV) festgelegt. Sie umfassen Sicherheit und Funktionstauglichkeit, Datenschutz und Informationssicherheit sowie Qualität und Interoperabilität. Die Erfüllung der Anforderungen wird mittels Checklisten in den Anlagen zur DiGAV und entsprechender Dokumentation nachgewiesen.

DiGA-Verordnung
DiGAV

8.4.1 Sicherheit und Funktionstauglichkeit

Der Nachweis der Produktsicherheit und Funktionstauglichkeit gilt durch die Konformitätsbescheinigung/CE Zertifikat der Benannten Stelle bzw. die Konformitätserklärung des Herstellers grundsätzlich als erbracht. Das heisst, medizinische Software, die nach den Anforderungen der MDR rechtmässig in Verkehr gebracht wurde, erfüllt diese Kriterien. Das BfArM führt hier generell keine weiteren Nachprüfungen durch.

8.4.2 Datenschutz

Die DiGAV ergänzt und konkretisiert Vorgaben zum Datenschutz aus der europäischen Datenschutz-Grundverordnung (DSGVO) sowie dem deutschen Bundesdatenschutzgesetz (BDSG) und dem Sozialgesetzbuch (SGB). Die Checkliste in Anlage 1 zur DiGAV beinhaltet dazu 40 Aussagen zur technischen Umsetzung und zur Orga-

nisation des Herstellers und dessen Prozessen. Insbesondere werden dabei die zulässigen Zwecke der Datenverarbeitung sowie die Zulässigkeit der Datenverarbeitung ausserhalb Deutschlands konkretisiert respektive eingeschränkt.

Zulässige Zwecke der Datenverarbeitung

Generell dürfen durch die Benutzung einer DiGA gewonnenen Daten nur aufgrund einer ausdrücklichen Einwilligung der Nutzer verarbeitet werden. Ausnahmen davon sind nur zulässig, wenn andere Rechtsvorschriften dies erlauben oder anordnen, z.B. zur Abrechnung des DiGA-Herstellers gegenüber der Krankenkasse und zur Erfüllung der Anforderungen der MDR (Rückverfolgbarkeit der Produkte, etc.). Daten dürfen zudem nur zu folgenden Zwecken verarbeitet werden:

- Zur Gewährleistung des bestimmungsgemässen Gebrauch der DiGA durch die Nutzer
- Zum Nachweis positiver Versorgungseffekte bei vorläufiger Aufnahme in das DiGA-Verzeichnis
- Zur Nachweisführung für Preisvereinbarungen zwischen Krankenkassen und DiGA-Herstellern
- Zur dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA

Die Verarbeitung von Daten zu anderen Zwecken, z.B. zu Werbezwecken, ist verboten.

Ort der Datenverarbeitung

Die Datenverarbeitung darf nur in Deutschland selbst, in Mitgliedsstaaten der EU und des EWR, in der Schweiz sowie in Drittstaaten mit vergleichbarem Schutzniveau (Angemessenheitsbeschluss nach Artikel 45 DSGVO) erfolgen. Eine Datenverarbeitung in den USA zum Beispiel ist nicht zulässig.

8.4.3 Informationssicherheit

Die DiGAV stellt auch konkrete Anforderungen an die Informationssicherheit, also an den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit sämtlicher über eine DiGA verarbeiteten Daten. Die Anforderungen richten sich dabei an Publikationen und Empfehlungen des Bundsamts für Sicherheit in der Informationstechnik (BSI) aus, insbesondere den BSI Standards 200-1, 200-2 und 200-3.

Zertifiziertes Managementsystem

Alle Hersteller von DiGAs müssen ein Managementsystem für Informationssicherheit (ISMS) nach ISO 27001 respektive BSI-Standard

200-2: IT-Grundschutz-Methodik implementieren und bei einer akkreditierten Stelle zertifizieren lassen. Dies beinhaltet insbesondere folgende Prozesse: - Schutzbedarfsanalyse: Kontinuierlicher Prozess zur Bestimmung der Schutzbedarfe von Daten, Anwendungen, Systemen etc. - Release-, Change- und Configuration-Management: Bewertung von Software-Updates und Releases in Bezug auf erforderliche Neubewertungen von Schutzmassnahmen, Risiken - Penetrationstests: Nachbildung möglicher Angriffsmuster um Sicherheitslücken festzustellen auf Basis der BSI Penetrationstests und OWASP Top-10 Sicherheitsrisiken. - Verzeichnis von genutzten Bibliotheken und Marktbeobachtung: Auflistung der in der DiGA verwendeten Produkte Dritter (einschließlich Open Source) und Prozess um sicherheitsrelevante, produktbezogene Informationen zu erhalten und zu bewerten	für Informationssicherheit (ISMS)
Die in den Checklisten (Anlage zur DiGAV) zur Datensicherheit aufgeführten Anforderungen sind direkt aus den Anforderungskatalogen des BSI-IT-Grundschutz abgeleitet. Insbesondere folgende Bausteine aus dem BSI-IT-Grundschutzkompendium sind zu berücksichtigen: - APP.1.4: Mobile Anwendungen (Apps) - APP.3.1: Webanwendungen - SYS.4.4: Allgemeines IoT-Gerät	BSI-IT-Grundschutzkompendium
Für DiGAs mit sehr hohem Schutzbedarf (bestimmt durch die Schutzbedarfsanalyse) müssen zudem weitergehende Massnahmen - wie Verschlüsselung der Daten auf Servern und 2-Faktor-Authentisierung beim Zugriff auf Gesundheitsdaten - getroffen werden.	DiGAs mit sehr hohem Schutzbedarf

8.4.4 Interoperabilität

Eine weitere Anforderung an DiGA ist die Interoperabilität. Interoperabilität ist die Eigenschaft technischer Systeme, auf technisch-syntaktischer (Austauschbarkeit von Daten über Netzwerke in bestimmten Datenformat), semantischer (übereinstimmendes Verständnis der Information bei Sender und Empfänger) und organisatorischer (gesellschaftlicher und gesetzlicher Rahmen) Ebene zusammenarbeiten zu können.

Die DiGAV legt dabei fest, welche Schnittstellen interoperabel sein müssen und wie dies durch die Nutzung von Standards realisiert werden muss.

Interoperable Schnittstellen

Insbesondere werden folgende interoperable Schnittstellen gefordert:

- Therapierelevante Auszüge der erhobenen Daten müssen in menschenlesbarer und ausdruckbarer Form bezogen werden können
- Erhobene Daten müssen in einem maschinenlesbaren, interoperablen Format bezogen werden können um von anderen digitalen Produkten verarbeitet werden zu können.
- Wenn die DiGA Daten aus anderen Medizinprodukten oder Sensoren (Wearables) bezieht, muss sie diese Geräte auch über eine interoperable Schnittstelle ansprechen können.

Die Schnittstellen können dabei redundant sein, d.h. es können neben den interoperabel gestalteten Schnittstellen auch andere bestehen, die den gleichen Zweck verfolgen.

Medizinische Informationsobjekte MIOs

Um die Interoperabilität einer Schnittstelle zu gewährleisten, können Hersteller auf sogenannte medizinische Informationsobjekte MIOs zurückgreifen. Das MIO DiGA Toolkit, eine modulare medizinische Datenstruktur, wird von der Kassenärztlichen Bundesvereinigung (KBV) bereitgestellt und weiterentwickelt. Grundsätzlich müssen interoperable Schnittstellen mithilfe solcher MIOs umgesetzt werden. Falls kein entsprechendes MIO vorhanden ist, können auch existierende offene, international anerkannte Schnittstellen- und/oder Semantikstandards benutzt werden (HL7, ISO, NEMA, etc.).

8.4.5 Weitere Qualitätsanforderungen

Nebst der Interoperabilität müssen DiGA auch weitere Qualitätsanforderungen erfüllen.

Robustheit

DiGAs müssen möglichst ohne Störungen, Datenverluste, Übertragungsfehler oder Schwierigkeiten bei der Verbindung mit Geräten genutzt werden können. Es muss unter anderem sichergestellt werden, dass Stromausfälle oder Unterbrechungen der Internetverbindung nicht zu Datenverlust oder -verfälschung führen. Eine Offline-Nutzbarkeit ist aber nicht vorgeschrieben. Externe Geräte und Sen-

soren müssen durch die DiGA, sofern möglich, auf ihre Funktionstüchtigkeit geprüft werden. Weiter sind auch Plausibilitätsprüfungen bei der Dateneingabe durch den Anwender vorgeschrieben.

Verbraucherschutz

Hersteller müssen die Anwender möglichst transparent über die Zweckbestimmung und Funktionalität der DiGA informieren. Auf Vertriebsplattformen müssen Kompatibilitätsaussagen zu Hard- und Software dargelegt werden und es muss klar ersichtlich sein, welcher Funktionsumfang die DiGA zur Verfügung stellt und welche Funktionen allenfalls dazugekauft werden müssen. In-App-Käufe von zusätzlichen, das heisst nicht zur DiGA gehörenden, Funktionen sind prinzipiell erlaubt, dürfen aber z.B. nicht in der DiGA beworben werden und es darf sich dabei nicht um sich automatisch verlängernde Abonnements oder zeitlich befristete Sonderangebote handeln.
Nutzerfragen müssen vom Hersteller zeitnah beantwortet werden. Konkret muss auf Anfragen innerhalb von 24 Stunden reagiert werden, idealerweise bereits mit einer Antwort.

Nutzerfreundlichkeit

Die Nutzerfreundlichkeit muss mittels Fokusgruppen-Tests evaluiert werden. Dabei müssen auch Teilnehmer miteinbezogen werden, die über wenig Vorerfahrung im Umgang mit digitalen Medien verfügen. Weiter müssen DiGAs zur Gewährleistung der Barrierefreiheit entweder Bedienhilfen für Menschen mit Einschränkungen beinhalten oder die durch die Plattform angebotenen Bedienhilfen unterstützen.

Unterstützung der Leistungserbringenden

Ist die DiGA für die gemeinsame Nutzung von Anwendern und Leistungserbringenden gedacht, muss der Hersteller klare Vorgaben machen, welche Rolle die Leistungserbringenden übernehmen, wie diese praktisch auszugestalten sind und welche rechtlichen Vorgaben dabei zu beachten sind.

Qualität medizinischer Inhalte

Die fachliche Grundlage einer DiGA muss aus akzeptierten und belastbaren Quellen (medizinischen Leitlinien, etablierten Lehrbüchern, veröffentlichten Studien, etc.) stammen. Diese Quellen müssen in der DiGA selbst offengelegt sein. Zudem muss der Hersteller, mittels geeigneter Prozesse, die Aktualität und Angemessenheit der fachlichen Grundlage kontinuierlich sicherstellen und Veränderungen in der weiteren Entwicklung der DiGA berücksichtigen (siehe dazu Kapitel 4.5 zu Post-Market Surveillance).

Auch an die Gewährleistung der Patientensicherheit stellt die DiGAV, neben der durch die CE-Kennzeichnung abgesicherten technischen Sicherheit, zusätzliche Anforderungen. Sie zielen insbesondere auf den bewussten Umgang mit bestehenden Restrisiken für die Anwender ab. So müssen z.B. Hinweise auf Risiken und geeignete Massnahmen zu deren Abschwächung oder Vermeidung gegeben werden. Kritische Messwerte oder Analyseergebnisse müssen von der DiGA erkannt werden und der Anwender muss entsprechend darauf hingewiesen werden (Hinweis auf Arztbesuch oder Empfehlung zum Abbruch respektive Veränderung der Nutzung der DiGA). Weiter müssen alle vom Nutzer eingegebenen oder über angebundene Medizingeräte oder Sensoren erhobenen Daten auf Konsistenzbedingungen geprüft werden.

Patientensicherheit

8.5 Nachweis positiver Versorgungseffekte

Für eine dauerhafte Aufnahme im DiGA Verzeichnis müssen die positiven Versorgungseffekte (pVE) einer DiGA mittels einer vergleichenden Studie nachgewiesen werden.

Positive Versorgungseffekte sind entweder ein medizinischer Nutzen (mN) oder patientenrelevante Struktur- und Verfahrensverbesserungen (pSVV) in der Versorgung. Medizinischer Nutzen ist definiert als eine Verbesserung des Gesundheitszustands, Verkürzung der Krankheitsdauer, Verlängerung des Überlebens oder eine Verbesserung der Lebensqualität. Patientenrelevante Struktur- und Verfahrensverbesserungen können erreicht werden in Bereichen wie Koordination der Behandlungsabläufe, Ausrichtung der Behandlung an Leitlinien und anerkannten Standards, Adhärenz, Erleichterung des Zugangs zur Versorgung, Patientensicherheit, Gesundheitskompetenz, Patientensouveränität, Bewältigung krankheitsbedingter Schwierigkeiten im Alltag oder Reduzierung der therapiebedingten Aufwände und Belastungen der Patienten und ihrer Angehörigen.

Positive Versorgungseffekte pVE

Positive Versorgungseffekte müssen immer in Bezug auf eine spezifische Patientengruppe (Indikation) nach ICD-10 Kodierung erfolgen. Eine DiGA kann zwar führ mehrere Indikationen eingesetzt werden, der Nachweis der pVE muss dann aber in der Regel für jede Patientengruppe gesondert geführt werden.

Eine Studie zum Nachweis positiver Versorgungseffekte muss generell belegen, dass die Anwendung der DiGA für Patienten besser ist als die Nichtanwendung. Die Studie muss also zeigen, dass für

Studie zum Nachweis der pVE

eine Patientengruppe, welche die DiGA im Rahmen der Behandlung nutzt, gegenüber einer Vergleichsgruppe, welche die DiGA nicht nutzt, ein pVE generiert wird (vergleichende Studie). Die Vergleichsgruppe kann dabei entweder eine Behandlung ohne Anwendung der DiGA erhalten, nicht behandelt werden, oder eine Behandlung mit einer anderen, vergleichbaren DiGA erhalten.

Die Studien können je nach untersuchten Endpunkten klinisch oder epidemiologisch sein, oder auch nach Methoden der Versorgungsforschung, der Sozialforschung oder der Verhaltensforschung etc. durchgeführt werden. Spezifische Anforderungen an Studientypen und Designs können dem DiGA Leitfaden des BfArM entnommen werden.

Die Studien müssen in Deutschland durchgeführt und in einem öffentlichen Studienregister registriert werden. Die Ergebnisse der Studie müssen spätestens 12 Monate nach Einreichung beim BfArM veröffentlicht werden.

Vorläufige Aufnahme zur Erprobung

Hersteller, die noch keine Studie zum Nachweis der pVE abgeschlossen oder begonnen haben, können eine vorläufige Aufnahme zur Erprobung im DiGA Verzeichnis beantragen. Dazu muss mittels systematischer Datenauswertung (Literaturrecherche und -bewertung sowie Auswertung von in der Anwendung der DiGA gewonnenen Daten) dargelegt werden, dass für eine bestimmte Patientengruppe ein pVE erzielt werden kann. Zudem muss der Hersteller ein Evaluationskonzept mit Studienprotokoll vorlegen. Das Evaluationskonzept muss dabei von einem unabhängigen wissenschaftlichen Institut erstellt werden, z.B. einer Clinical Research Organisation (CRO).

9 MedTech Glossar für den App Entwickler

9.1 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
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

9.2 Behörden, Vereinigungen etc.

Schweizerisches Heilmittelinstitut, Zulassungs- und Kontrollbehörde für Heilmittel in der Schweiz	Swissmedic
Koordinierungsgruppe Medizinprodukte / Medical Device Coordination Group (MDCG)	MDCG
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

9.3 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 Electrotechnical Commission, Normenorganisation im Bereich Elektronik und Elektrotechnik (z.B. IEC 60601-X)	IEC
Unique Device Identifier, 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 Market Surveillance (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
Grundlegende Sicherheits- und Leistungsanforderungen. Anhang I der MDR	GSPR
Kurzbericht über Sicherheit und klinische Leistung (engl. *Summary of safety and clinical performance*, SSCP)	SSCP
Regelmässig aktualisierter Bericht über die Sicherheit (engl. *Periodic safety update report,* PSUR)	Sicherheitsbericht PSUR

10 Wichtige Ressourcen, Leitfäden etc.

Swissmedic – Informationen zur Medizinprodukte-Regulierung	Informationen Swissmedic
Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 (Blue Guide)	Blue Guide
MEDDEV-Dokumente (MDD)	Guidance documents MEDDEV
MDCG-Dokumente (MDR)	Guidance Documents MDCG
Auflistung aller Benannten Stellen mit Akkreditierung nach MDR	Liste der Benannten Stellen MDR
Schweizer Normenverband	Swiss Standards SNV
BfArM - Information zum Inverkehrbringen von Medizinprodukten	Im Überblick: Inverkehrbringen von Medizinprodukten
BfArM – Digitale Gesundheitsanwendungen DiGA	DiGA

10.1 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/