Spitzenverband Digitale Gesundheitsversorgung

IM FOKUS: REGULATORISCHE ANFORDERUNGEN AN DIGA

Mit der Einführung Digitaler Gesundheitsanwendungen (DiGA) vor fast zwei Jahren wurde auch ein komplett neues Zulassungsverfahren etabliert. Das erfolgreiche Durchlaufen dieses Verfahrens ist Voraussetzung für die Aufnahme einer DiGA in den Leistungskatalog der Gesetzlichen Krankenversicherungen. Entgegen einer gängigen Kritik, die Anforderungen an DiGA seien zu gering, müssen DiGA-Hersteller die Einhaltung hoher Standards nachweisen.
Im zweiten Teil unserer Serie „Im Fokus" wollen wir diese umfangreichen Anforderungen genauer unter die Lupe nehmen: Was steckt hinter den Vorgaben, Zahlen und ISO-Normen, mit denen Hersteller Sicherheit, Funktionstauglichkeit oder Datenschutz ihrer DiGA belegen müssen?

Anforderungen der Medizinprodukteverordnung (MDD) / Medizinprodukterichtlinie (MDR)

Da jede DiGA als Medizinprodukt zertifiziert bzw. registriert sein muss, sind die Anforderungen der Medizinprodukteverordnung (MDD) oder der neuen Medizinprodukterichtlinie (MDR) zu erfüllen.

Dazu gehören unter anderem:

- Die Implementierung eines Qualitätsmanagementsystems gemäß ISO 13485
  Hersteller von Medizinprodukten müssen laut MDR ein Qualitätsmanagementsystem (QMS) haben. Durch das QMS wird sichergestellt, dass alle Vorschriften eingehalten und Verbesserungen, Effektivität und Sicherheit stets gefördert werden. Es umfasst jeden Aspekt des Unternehmens, der einen Einfluss auf die Qualität des Produkts hat (z.B. Produktentwicklung, Zuliefererauswahl, Kommunikation mit Anwender:innen und Verordner:innen).

- Die Einführung eines Risikomanagements gemäß ISO-14971
  Das Risikomanagement ist ein wichtiger Teil der gesamten Medizinprodukte-Zulassung. In aufwändigen Verfahren wie einer Preliminary Hazard Analysis (PHA) oder einer Failure-Mode and Effects Analysis (FMEA) werden mögliche Risiken identifiziert und genauer untersucht. Anschließend werden die Risiken bestmöglich bewertet und minimiert. Jedes Unternehmen benötigt hierfür mindestens eine:n Risikomanager:in. Diese:r muss nicht nur einmalig, sondern dauerhaft die Risiken des Medizinprodukts überwachen, Studien-Datenbanken durchsuchen und auf Rückmeldungen aus dem operativen Betrieb reagieren.

- Der Nachweis der Gebrauchstauglichkeit gemäß IEC-62366
  Die Gebrauchstauglichkeit nach IEC-62366 soll sicherstellen, dass die entwickelten Produkte von der Zielgruppe tatsächlich verstanden und korrekt angewendet werden können. Um die Gebrauchstauglichkeit nachzuweisen, müssen Hersteller beispielsweise Expert:inneninterviews führen oder Usability-Test durchführen und nachweisen.

- Das Aufsetzen eines Softwareentwicklungs-Prozesses gemäß IEC-62304 und IEC-82304
  Die Produktentwicklung einer Medizinprodukt-App muss Normvorgaben mit Anforderungen der Stakeholder zusammenbringen und diese in eine sinnvolle Produktarchitektur überführen. Es ist ein komplexer Software-Entwicklungsprozess erforderlich, der strengen Vorgaben genügen und genauestens dokumentiert werden muss. Jede DiGA muss zunächst einer Software-Sicherheitsklasse zugeordnet und im Rahmen eines detaillierten Software-Entwicklungsplans entwickelt werden. Die verwendete Software ist prozessual zu überprüfen und es müssen Software-Tests in verschiedenen Teststufen beschrieben und dokumentiert werden.

- Das Bereitstellen eines Vigilanz-Prozesses
  Medizinprodukthersteller sind verpflichtet, ein Vigilanz-System aufzubauen, das den Schutz und die Gesundheit von Patient:innen gewährleisten soll. In der Praxis bedeutet dies, dass Hersteller zügig reagieren müssen, falls ihr Produkt nicht wie erwartet funktioniert und eine Gefahr für den Nutzer oder die Nutzerin besteht.

- Ein Post Market Surveillance-System
  Die Post Market Surveillance (PMS) verpflichtet Hersteller auch nach der Markteinführung ihres Produktes zu einer Marktüberwachung: Sie müssen aktiv überprüfen, ob ihr Produkt zu Komplikationen führt oder ob ähnliche Produkte zu Nebenwirkungen führen können. Die Reaktion auf etwaige Vorfälle ist bereits im Vorfeld für die Mitarbeitenden festzulegen.

Neben den hohen Anforderungen aus der MDR bzw. der MDD ergeben sich aus der Digitale Gesundheitsanwendungen-Verordnung (DiGAV) und dem SGB V weitere Anforderungen an DiGA-Hersteller.

Anforderungen aus der Digitale Gesundheitsanwendungen-Verordnung (DiGAV)

Die nachfolgenden Anforderungen skizzieren einen kleinen Teil der insgesamt 120 Einzelkriterien, die Hersteller für eine Listung im BfArM-Verzeichnis erfüllen müssen:

- Informations-Sicherheits-Management-System (ISMS) gemäß ISO-27001
  Seit dem 1. April 2022 müssen Hersteller ein ISMS-System gemäß ISO-Norm vorweisen. Damit wird nicht nur das Produkt, sondern das gesamte Unternehmen einer Sicherheitsüberprüfung unterzogen. Es werden alle Prozesse, sämtliche materiellen und immateriellen Werte und Mitarbeitenden einbezogen. Das gesamte System wird durch eine:n unabhängige:n und bei der Deutschen Akkreditierungsstelle akkreditierten Prüfer:in in mehrtägigen Audits überprüft und muss regelmäßig rezertifiziert werden.

- Datensicherheit
  Bereits im DiGA-Antrag müssen Hersteller nachweisen, welche Maßnahmen zur Datensicherheit ergriffen werden - dies sind 39 vom Gesetzgeber klar definierte

Anforderungen. Dazu gehören beispielsweise Penetrations-Tests, also simulierte “Hacker-Angriffe”, die die Software auf Schwachstellen überprüfen und bestmöglich auf Cyber-Angriffe vorbereiten soll. Durchgeführt werden diese von darauf spezialisierten Firmen.

- Datenschutz-Vorgaben
  Die Datenschutz-Vorgaben für Digitale Gesundheitsanwendungen gehen weit über die Vorgaben der Datenschutzgrundverordnung (DSGVO) hinaus. Insgesamt handelt es sich um 40 weitere gesetzlich definierte Anforderungen. Hierzu zählen insbesondere Angaben zum Umgang mit personenbezogenen Daten sowie Gesundheitsdaten und der explizite Nachweis, in welcher Form Daten gespeichert und verarbeitet werden.

Weitere Anforderungen aus dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG), die DiGA zukünftig zusätzlich erfüllen müssen:

- Datensicherheits-Zertifizierung gemäß BSI:
  Derzeit liegen drei technische Richtlinien des Bundesamt für Sicherheit in der Informationstechnik (BSI) vor: für Mobile Anwendungen (151 Prüfaspekte), für Webanwendung (106 Prüfaspekte) sowie für Hintergrundsysteme allgemein (106 Prüfaspekte). Das BSI muss bis zum 31. Dezember 2022 im Einvernehmen mit dem BfArM die nachzuweisenden Anforderungen an die Datensicherheit festlegen - erst dann können die Hersteller mit der Umsetzung starten.

- Datenschutz-Zertifizierung
  Ab 2024 ist eine Zertifizierung des Datenschutzes erforderlich, die zusätzlich zu den Anforderungen an den Datenschutz aus dem DiGA-Antragsverfahren, den Maßnahmen der ISMS-Zertifizierung und den datenschutzrechtlichen Prüfaspekten der Datensicherheits-Zertifizierung gemäß BSI durchgeführt werden muss. Vorgaben hierzu wurden kürzlich vom BfArM veröffentlicht.*

Fazit

DiGA sind digitale Lösungen, die sich durch die regulatorischen Anforderungen von ungeprüften Gesundheitsapps unterscheiden und Qualität, Sicherheit, Datenschutz, Nutzerfreundlichkeit uvm. gewährleisten müssen.
Entscheidend ist, dass zukünftige Anforderungen nicht dazu führen, dass Patient:innen von der Nutzung ausgeschlossen werden. Auch der Weg zur Nutzung einer DiGA sollte diesem Prinzip entsprechen: von der Ausgabe des Rezepts, über die Freischaltung bis hin zur Anmeldung im Programm. All das muss einfach durchführbar sein – unabhängig von der technischen Affinität der Nutzer:innen und dem Alter der Geräte, die sie benutzen. Zukünftige Kriterien an digitale Gesundheitsanwendungen müssen dies zwingend berücksichtigen. Nur wenn DiGA für alle Patient:innen einfach zugänglich und nutzbar sind, können sie den größtmöglichen Beitrag zur Verbesserung der Versorgungsqualität leisten.

*https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html 1