Fragenkatalog „IT-Sicherheit bei Medizinprodukten“

(Version 4, Stand: 03.12.2021)

Vorbemerkungen:

- Dieses Dokument wurde durch die Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland (IG-NB) erstellt und soll den Benannten Stellen, Herstellern und interessierten Dritten als Orientierung dienen.
- In diesem Dokument werden zentrale Fragen bei der Bewertung der IT-Sicherheit von Medizinprodukten aufgeworfen sowie Verweise auf die wesentlichen Gesetze und Normen gegeben. Das Dokument soll regelmäßig überarbeitet und an den aktuellen Stand der Normen angepasst werden.
- Das Dokument erhebt keinen Anspruch auf Vollständigkeit oder verpflichtende Anwendung.
- Die Schwerpunkte der Bewertung ergeben sich aus der Zweckbestimmung.
- Dieser Fragenkatalog basiert in Teilen auf dem „Leitfaden IT-Sicherheit für Medizinprodukte“ von TÜV SÜD, Johner Institut sowie Dr. Georg Heidenreich (https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md)
- Fragen hinsichtlich der Security-Risiken künstlicher Intelligenz finden sich im „Fragenkatalog Künstliche Intelligenz bei Medizinprodukten“ der IG-NB.

Referenzen:

- Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte (93/42/EWG)
- Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (2017/745/EU)
- Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (2017/746/EU)
- DIN EN ISO 13485:2016-08 Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke (ISO 13485)
- DIN EN ISO 14971:2013-04 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971)
- DIN EN 60601-1:2013-12 Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale (IEC 60601-1)
- DIN EN 62304:2016-10 Medizingeräte-Software - Software-Lebenszyklus-Prozesse (IEC 62304)
- DIN EN 62366:2008-09 Medizinprodukte - Anwendung der Gebrauchstauglichkeit auf Medizinprodukte (IEC 62366)
- ISO/TR 80002-2:2017-06 Medizinische Gerätesoftware - Teil 2: Validierung von Software zur Verwendung in der Qualitätssicherung für medizinische Geräte (ISO TR 80002-2)
- DIN EN 82304-1:2018-04 Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit (IEC 82304)

Inhalt:

A) Allgemeine Anforderungen

1. Kompetenzen

1.	Verfügt der Hersteller über angemessene Aufzeichnungen über die Ausbildung, Weiterbildung und Kompetenzen, die den Schluss erlauben, dass die Personen tatsächlich über diese Kompetenzen (mit Blick auf Cyber-Security) verfügen? Wie stellt die Organisation Kompetenzanforderungen bezüglich der IT-Sicherheit dar?	• ISO 13485, 6.2. • ISO 14971, 3.3.
2.	Erfolgt die Einbindung externer Kompetenzen gemäß den Regelungen zu ausgelagerten Prozessen? Wie wird die Kompetenz ausgelagerter Personen aufgezeichnet/dokumentiert?	• ISO 13485, 4.1.5. und 7.3.2.

2. Dokumentation

1.	Hat der Hersteller die Erfüllung der Cyber-Security-Anforderungen als Bestandteil der Grundlegenden Anforderungen dokumentiert?	• 2017/745/EU, Anhang 1, 17.2. und 17.4. • 2017/746/EU, Anhang I, 16.2. und 16.4. • (93/42/EWG, Artikel 3) • ISO 13485, 7.3.6. und 7.3.7.

B) Anforderungen an die Prozesse

1. Anforderungen an die Produktentwicklung

a) Zweckbestimmung und Stakeholder-Anforderungen

1.	Hat der Hersteller alle Nachbarsysteme (Medizinprodukte, IT-Systeme) bestimmt, die mit dem Produkt verbunden werden dürfen?	• 2017/745/EU, Anhang I, 14.1. und 14.2. (d) • 2017/746/EU, Anhang I, 13.1. und 13.2. (d) • (93/42/EWG, Anhang I, 9.1. und 13.6. (c)) • IEC 82304-1, 4.1. (b) und 4.2. (d)
2.	Hat der Hersteller die vorgesehene Nutzungsumgebung (Hard- und Software) festgelegt?	• IEC 60601-1, 14.13. • IEC 62304, 5.2.2. • IEC 82304-1, 4.1. und 4.2.
3.	Hat der Hersteller die Risiken (Gefährdung) analysiert (mit Blick auf die spezifizierten Nutzer) und die Umgebung? Wie wird unberechtigter Zugriff verhindert? Wie wird eine Verwendung in einer nicht-spezifizierten Umgebung verhindert?	• 2017/745/EU, Anhang I, 14.2. (d) • 2017/746/EU, Anhang I, 13.2. (d) • IEC 82304-1, 4.1. (c)
4.	Hat der Hersteller im Risikomanagement beschrieben, welche Bedrohungen für die IT-Sicherheit bestehen und welche Gefährdungen für die Patienten, Anwender und Dritte daraus entstehen?	• IEC 62304, 7.1.2.
5.	Hat der Hersteller jedes Benutzungsszenario untersucht und welche Risiken sich aus einer nicht spezifizierten Anzeige von Informationen (z.B. keine, falsche, zu späte Anzeige) ergeben?	• IEC 62366-1, 5.3. und 5.4.
6.	Hat der Hersteller für jede Datenschnittstelle die verwendeten Protokolle und Standards spezifiziert?	• IEC 62304, 5.2.2. • IEC 82304-1, 4.2. (b)

b) System- und Software-Anforderungen

i) Authentifizierung und Autorisierung

1.	Hat der Hersteller die Angemessenheit des Authentifizierungsverfahrens (Benutzername/Passwort, Biometrisches Verfahren, Token (z.B. Karte) etc.) für alle Rollen und alle Nachbarsysteme begründet?	• ISO 14971, 6.6.
2.	Hat der Hersteller im Risikomanagement die Auswirkungen für die Patientensicherheit analysiert, wenn eine Person nicht auf Patienten- oder Gerätedaten zugreifen kann (z.B. keine Berechtigung, Passwort vergessen), und entsprechende Maßnahmen definiert?	• ISO 14971, 6.6.

ii) Daten, Kommunikation

1.	Hat der Hersteller alle vom System verwalteten Daten identifiziert?	• IEC 62304, 5.5.2. (b) und 5.5.2. (e)
2.	Hat der Hersteller die Schutzwürdigkeit dieser Daten mit Bezug zur Vertraulichkeit und deren Auswirkung auf die Patientensicherheit bewertet?	• IEC 62304, 7.1.2.
3.	Hat der Hersteller im Risikomanagement die Auswirkungen bewertet, wenn der Schutz besonders schützenswerter Daten nicht mehr gegeben ist?	• IEC 62304, 7.1.2.
4.	Hat der Hersteller im Risikomanagement die Folgen einer Überlastung des Systems durch zu viele Anfragen (z.B. DoS (Denial of Service)) oder Anfragen mit zu großen Daten-Volumina untersucht und falls notwendig Maßnahmen definiert?	• 2017/475/EU, Anhang I, 14.2. (d) und 17.2. • 2017/476/EU, Anhang I, 13.2. (d) und 16. • IEC 82304-1, 4.2.10. und 4.5. (e)
5.	Hat der Hersteller im Risikomanagement die Folgen analysiert, wenn das Netzwerk nicht mehr oder nicht mehr in der erwarteten Güte zur Verfügung steht?	• 2017/745/EU, Anhang I, 17.4. • 2017/746/EU, Anhang I, 16.4. • IEC 60601-1, 14.13.
6.	Hat der Hersteller im Risikomanagement die Folgen eines Datenverlusts analysiert und ggf. Maßnahmen festgelegt (z.B. Backup und Wiederherstellung von Daten)?	• IEC 60601-1, 4.3.
7.	Wie stellt der Hersteller sicher, dass externe Daten vor der Verarbeitung auf Validität geprüft werden?	• 2017/745/EU, Anhang I, 14.1., 14.2. (d) und 18.8. • 2017/746/EU, Anhang I, 13.1. und 13.2. (d)

iii) Patches

1.	Hat der Hersteller einen Deployment-Prozess für Updates, Patches, usw. etabliert? Beinhaltet dieser die Fragestellung, wer Patches einspielen darf?	• IEC 62304, 6.
2.	Wie ist die Schnittstelle zur Vigilanz definiert?	• IEC 62304, 6.1. (b)
3.	Verfügt der Hersteller über eine Liste aller SOUP-/OTS-Komponenten?	• IEC 62304, 8.1.2.

iv) Sonstiges

1.	Welche Maßnahmen sind implementiert, um Angriffe auf die IT-Sicherheit bzw. die Kompromittierung der IT-Sicherheit zu erkennen?	• IEC 62304, 5.2.3. und 5.2.4. • IEC 82304-1, 4.5. (f)
2.	Hat der Hersteller abgeschätzt, welche Funktionalität das Medizinprodukt auch im Falle einer Kompromittierung der IT-Sicherheit gewähren muss (wesentliche Leistungsmerkmale)?	• IEC 60601-1, 4.3. • IEC 82304-1, 4.5. (g)

c) System- und Software-Architektur

1.	Hat der Hersteller alle SOUP-/ OTS-Komponenten dokumentiert (inkl. Version, Hersteller, Referenz auf Informationen zu Updates, Release-Notes)?	• IEC 62304., 8.1.2
2.	Hat der Hersteller die spezifischen Risiken, die sich durch die Wahl der Technologien (insbesondere Programmiersprache, SOUP-/OTS-Komponenten inklusive Betriebssystemen) ergeben, analysiert? Aktualisiert er diese Analyse fortlaufend? Wurden plattformspezifische Faktoren (z.B. Speicherleaks C++; Android, …) betrachtet? Wie hält sich der Hersteller bezüglich dieser spezifischen Risiken auf dem Laufenden?	• ISO 13485., 8.3 • IEC 62304., 5.3.3., 5.1.7., 7.1.3. und 8.1.2. • IEC 82304-1, 4.7. und 8.2.
3.	Hat der Hersteller Maßnahmen ergriffen, um sicherzustellen, dass die verwendeten Werkzeuge (z.B. Entwicklungsumgebung, Compiler), sowie die Plattformen und SOUP-/OTS-Komponenten frei von Schadcode sind?	• ISO 13485, 4.1.6. und 7.5.6. • ISO TR 80002-2
4.	Hat der Hersteller eine Liste aller Dienste erstellt, die das Produkt (z.B. durch sein Betriebssystem) nach "außen" anbietet bzw. nutzt?	• 2017/745/EU, Anhang I, 4. (a) • 2017/746/EU, Anhang I, 4. (a) • (93/42/EWG,

		Anhang I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.
5.	Hat der Hersteller für jeden Dienst begründet, weshalb dieser (zeitlich unbeschränkt) nach außen sichtbar sein muss?	• 2017/745/EU, Anhang I, 4. (a) • 2017/746/EU, Anhang I, 4. (a) • (93/42/EWG, Anhang I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.
6.	Wenn das Produkt eine Schnittstelle anbietet, hat der Hersteller im Risikomanagement beschrieben, wie Angriffe über diese Schnittstelle beherrscht werden?	• 2017/745/EU, Anhang I, 4. (a) • 2017/746/EU, Anhang I, 4. (a) • (93/42/EWG, Anhang I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.
7.	Hat der Hersteller für jede Rolle und jedes Nachbarsystem die Funktionen des Produkts bestimmt, auf die sie über die jeweilige Schnittstelle zugreifen darf?	• IEC 82304-1, 7.2.3.2. (c)
8.	Hat der Hersteller für jeden nach außen sichtbaren Dienst den Prozess identifiziert, der diesen Dienst anbietet / realisiert?	• IEC 62304, 5.3.
9.	Hat der Hersteller festgelegt, wie das Produkt eine Kompromittierung der IT-Sicherheit feststellt, diese dokumentiert (log-file) und wie es darauf reagiert?	• IEC 82304-1, 4.5. (f)
10.	Hat der Hersteller für alle Software-Komponenten, Dienste bzw. Prozesse, Daten und Software-Komponenten analysiert, welche Risiken entstehen, wenn diese sich aufgrund eines Problems mit der IT-Sicherheit nicht spezifikationsgemäß verhalten?	• IEC 60601-1, 14.13. • IEC 62304, 7.1.2. • IEC 82304-1, 7.2.3.2.
11.	Hat der Hersteller die Software-Anforderungen in der Software-Architektur berücksichtigt?	• IEC 62304, 5.3.1.

d) Implementierung und Erstellung der Software

1.	Hat der Hersteller Coding-Guidelines erstellt, die Anforderungen spezifisch für die IT-Sicherheit stellen?	• IEC 62304, 5.1. und 5.5.3.
2.	Hat der Hersteller entweder die Software (Source-Code und Binaries) vor der Auslieferung auf Schadcode überprüft und/oder hat er alle an der Entwicklung und "Produktion" der Software beteiligten Rechner gegen Malware geschützt (Integrität des Verteilungsweges)? Wie wird sichergestellt, dass Installationspakete vor Installation nicht unrechtmäßig verändert werden (Integrität des Vertriebsweges, z.B. durch Prüfsummen, Signierung, …)?	• IEC 62304, 5.8.8.

e) Bewertung von Software-Einheiten

1.	Wie stellt der Hersteller sicher, dass IT-Sicherheit bei der Entwicklung der Software-Einheiten berücksichtigt worden ist (security-by-design)?	• IEC 62304, 5.1.1. und 5.5.3.

f) System- und Software-Tests

1.	Hat der Hersteller eine adäquate Beschreibung der Auswahl und Angemessenheit von Tests bezüglich Einhaltung der Anforderungen der im Risikomanagement definierten Maßnahmen zur Cybersicherheit dokumentiert, die die Wirksamkeit der Kontrollmaßnahmen bestätigen?	• ISO 14971, 6.2. und 6.3.
2.	Hat der Hersteller im Testplan die Überprüfung aller System-/Software-Anforderungen vorgesehen?	• IEC 62304, 5.1.1. (c) und 5.1.6.

g) Produktfreigabe

1.	Hat der Hersteller die notwendigen Pläne für die der Entwicklung nachgelagerten Phase bezüglich IT-Sicherheit (z.B. Post-Market und Incident Response Plan, inkl. SOUP) erstellt?	• 2017/475/EU, Kapitel VII • 2017/476/EU, Kapitel VII • ISO 13485, 8.2.1. und 8.2.2. • IEC 62304, 6 und 7.1.3.
2.	Hat der Hersteller die Vollständigkeit der Tests geprüft und die Tests mit den Anforderungen verknüpft?	• IEC 62304, 5.8.1 und 5.8.6. • IEC 82304-1, 6.

2. Anforderungen an die Entwicklung nachgelagerten Phasen

a) Produktion, Distribution, Installation

1.	Hat der Hersteller beschrieben, wie sichergestellt ist, dass nur genau die vorgesehenen Artefakte (Dateien) in genau der vorgesehenen Version im Produkt oder als Produkt ausgeliefert werden?	• IEC 62304, 5.8.8.
2.	Hat der Hersteller beschrieben, wie die für die Installation verantwortlichen Personen das Wissen erlangen können, welches die aktuellste Version ist und wie Verwechslungen bei der Installation ausgeschlossen werden können?	• ISO 13485, 7.8.3. und 8.3. • IEC 62304, 5.8.4.
3.	Hat der Hersteller beschrieben, wie bei der Installation sichergestellt wird, dass die Anforderungen, die in den Begleitmaterialien spezifiziert sind, tatsächlich erfüllt sind?	• ISO 13485, 7.5.3.
4.	Hat der Hersteller Verfahren etabliert, die gewährleisten, dass er mit den Betreibern und Anwendern seiner Produkte zeitnah kommunizieren kann?	• ISO 13485, 7.2.3. und 8.3.3. • IEC 82304-1, 8.4.
5.	Hat der Hersteller Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen, einschließlich Schutz vor unbefugtem Zugriff, festgelegt und kommuniziert?	• 2017/745/EU, Anhang I, 17.4. • 2017/746/EU, Anhang 1, 16.4.

b) Marktüberwachung

1.	Hat der Hersteller einen Post-Market Surveillance Plan erstellt, der auch IT-Sicherheitsthemen angemessen adressiert? - Hat der Hersteller beschrieben, welche Informationen aus der nachgelagerten Phase gesammelt werden, insbesondere zu zusätzlich versuchter oder erfolgreicher Kompromittierung? - Hat der Hersteller beschrieben, wie und über welche Kanäle Informationen aus der nachgelagerten Phase gesammelt werden? - Hat der Hersteller beschrieben, wie Informationen aus der nachgelagerten Phase ausgewertet bzw. bewertet werden? - Hat der Hersteller beschrieben, welche Maßnahmen daraus resultieren? - Hat der Hersteller für jede SOUP-/OTS-Komponente mindestens eine Quelle und die Frequenz für deren Überwachung festgelegt, über die er über IT-Sicherheitsbezogene Probleme informiert wird? Hat er beschrieben, welche Rolle mit welchen Werkzeugen diese Auswertung vornimmt? - Hat der Hersteller beschrieben, wie er überwacht, dass verwendete Technologien und Verfahren (z.B. Kryptologie) noch sicher sind?	• 2017/745/EU, Kapitel VII • 2017/746/EU, Kapitel VII • (93/42/EWG, Artikel 10)

c) Incident Response Plan

1.	Ist das IT-Security-Incident-Handling des Herstellers geeignet, innerhalb kürzester Zeit auf Notfälle zu reagieren?	• 2017/745/EU, Artikel 87

		• 2017/746/EU, Artikel 82 • (93/42/EWG, Artikel 10) • IEC 82304-1, 8.4.

d) Außerbetriebnahme

1.	Existiert ein Lifecycle-Konzept für Patientendaten (welches den Schutz vor ungewollter Löschung sowie die Nutzungsänderung und endgültige Löschung einschließt)?	• IEC 82304-1, 8.5.

C) Anforderungen an das Produkt

Vorbemerkung:
Es folgen Fragestellungen zu einer möglichen Umsetzung. Auf Gesetzes- und Normenverweise wurde verzichtet, da die Fragestellungen aus den Anforderungen an die Prozesse (Kapitel B) resultieren.

1. System-/Software-Anforderungen

a) Authentifizierung

1.	Ist sichergestellt, dass keine Default-Passwörter zur Anwendung kommen?
2.	Zeigt das Produkt im Falle eines nicht erfolgreichen Logins nur Informationen an, die es dem Anwender nicht erlauben, die genaue Ursache der Sperrung zu erkennen, wie z.B. Meldungen „falscher Benutzername“ oder „falsches Passwort“?
3.	Hat der Hersteller ein Konzept für Berechtigungen und ggf. Rollen für Anwender und Nachbarsysteme aufgestellt?
4.	Sofern vorhanden: Erlaubt das Produkt jeder Rolle den Zugriff auf nur die Funktionen, für die sie berechtigt ist? (Dies gilt insbesondere auch für das Update/Upgrade des Produkts.)
5.	Erlaubt das Produkt berechtigten Benutzern, andere Benutzer und Nachbarsysteme zu sperren? Hat der Hersteller risikobasierte Maßnahmen festgelegt, die dazu führen, dass keine Safety-Risiken entstehen?
6.	Werden in einer Client-Server Architektur alle Maßnahmen zur IT-Sicherheit serverseitig berechnet und geprüft? Werden in einer Client-Server Architektur alle Eingaben des Clients serverseitig geprüft?

b) Kommunikation und Speicherung

1.	Wie stellt der Hersteller die Integrität und Vertraulichkeit von Daten im Falle ihrer Übermittlung sicher?
2.	Wie wird die Nutzungsänderung oder ungewollte Löschung von Daten verhindert?
3.	Wenn Daten endgültig gelöscht werden sollen, wie wird sichergestellt, dass das auch passiert?
4.	Lehnt das Produkt per Default anwendungs- und risikobezogen alle unbekannten eingehenden Verbindungen (z.B. USB, TCP, Bluetooth) ab?
5.	Überprüft das Produkt alle Benutzereingaben und alle eingehenden Daten vor der weiteren Verarbeitung anhand vom Hersteller festgelegter Überprüfungskriterien?
6.	Speichert das Produkt Passwörter so, dass sie nicht rekonstruiert werden können?
7.	Hat der Hersteller einen Schutz für personenidentifizierende Merkmale definiert und umgesetzt?
8.	Hat der Hersteller Maßnahmen implementiert, um die Integrität von Software und Daten aufrechtzuerhalten?
9.	Erlaubt es das Produkt Datenschnittstellen zu deaktivieren?
10.	Existiert eine Liste aller Empfänger, an die Daten übermittelt werden, mit genauer Angabe der Art der Daten und eventuell zu erfolgender Anonymisierung/Pseudonymisierung?
11.	Wurde identifiziert, welche Daten (z.B. Google Werbe-ID) ggf. zu einer De-Pseudonymisierung

	führen könnten? Wie wird dem vorgebeugt?
12.	Wie ist sichergestellt, dass der Nutzer über die Speicherinhalte und -orte seiner Daten informiert ist und diesen vor einer ersten Übermittlung (dokumentiert) zustimmt?
13.	Hat der Nutzer die Möglichkeit, bestimmten Übermittlungen zu widersprechen?
14.	Ist der Nutzer über Datenweitergaben jedweder Art zu Speicherorten, die nicht den EU-Datenschutzbestimmungen unterliegen, informiert und stimmt einer Speicherung ausdrücklich auch an diesen Orten zu?
15.	Was passiert bei einem Widerruf/einer Nichtzustimmung?
16.	Ist im Risikomanagement definiert, zu welchen Folgen eine Kompromittierung jedes einzelnen Datenspeicherorts führt und welche Maßnahmen getroffen werden, dies zu verhindern?“

c) Patches

1.	Existiert ein System, das es erlaubt Patches aufzuspielen und fehlerhafte Patches zu entfernen?
2.	Gibt es einen Integritäts-Check der Patches?

d) Sonstiges

1.	Hat der Hersteller bezüglich log-files festgelegt, wo die Daten liegen, wie diese geschützt, aktualisiert und in welcher Form sie (automatisiert) ausgewertet werden können?
2.	Existiert ein risikobasiertes Logging-Konzept, welches wesentliche Änderungen am Produkt und Ereignisse mitschreibt und vor Veränderungen schützt?

2. System-/Software-Architektur

1.	Verwendet die Software für alle kryptographischen Funktionen (z.B. Verschlüsselung, Signierung) ausschließlich bewährte Bibliotheken / Komponenten oder ist eine Eigenimplementation umfassend bewertet?
2.	Basiert die Software auf den Versionen der SOUP-/OTS-Komponenten, die keine sicherheitsrelevanten Schwachstellen enthalten? Sind Ausnahmen begründet?

3. Begleitmaterialien

1.	Legt die Gebrauchsanweisung die vorgesehene IT-Umgebung für den Betrieb fest?
2.	Legt die Gebrauchsanweisung fest, welche Aktivitäten die Betreiber wie und wie häufig durchführen müssen?
3.	Legen die Installations- und Service-Anleitungen fest, welche weiteren Rollen (Betreiber, Service-Techniker) welche Aktivitäten wie häufig durchführen müssen?
4.	Beschreiben die Begleitmaterialien, wie mit verlorengegangenen oder gestohlenen Authentifizierungs-Elementen (z.B. Karten, Zertifikaten, kryptographischen Schlüsseln) sowie mit vergessenen Passwörtern umgegangen werden soll?
5.	Beschreiben die Begleitmaterialien, wie die Anwender erkennen können, dass das Produkt ein Problem mit der IT-Sicherheit hat, und wie sie sich in diesem Fall verhalten sollen?

6.	Beschreiben die Begleitmaterialien, welche Anti-Malware-Software für das Produkt zugelassen und von wo (z.B. Link) diese zu beziehen ist und wer für deren Aktualisierung verantwortlich ist?
7.	Enthalten die Begleitmaterialien die Kontaktdaten des Herstellers, über die dieser z.B. bei Problemen mit der IT-Sicherheit zu erreichen ist?
8.	Beschreiben die Begleitmaterialien das Produkt auch technisch?

D) Ergänzende Aspekte die im Rahmen des Risikomanagements durch den Hersteller zusätzlich adressiert werden sollen

1. System- und Software-Architektur

(Ergänzung zu ISO 14971, Anhang C)

1.	Hat der Hersteller für jeden Prozess den Nutzer (auf Betriebssystemebene) identifiziert und begründet, wenn dieser nicht mit minimalen Rechten ("worst case" als Root) läuft?
2.	Hat der Hersteller Risiken durch mangelnde IT-Sicherheit systematisch durch ein Threat-Modeling abgeleitet?
3.	Hat der Hersteller die Risiken analysiert, die sich durch das (Auto-)Update von Anti-Malware ergeben?
4.	Sind die ggf. enthaltenen FPGAs Teil der Risikoanalyse?
5.	Wird der FPGA-Code, der als IP core bezogen wird, wie Bibliotheken gelenkt?
6.	Sind Update-Möglichkeiten für FPGAs vorgesehen, die im Rahmen der Risikoanalyse als sicherheitsrelevant eingestuft wurden?

2. Produktfreigabe

1.	Hat der Hersteller die häufigsten Schwachstellen und daraus resultierende Gefährdungen in der Risikoanalyse adressiert und kann darlegen, weshalb diese Risiken beherrscht sind?
2.	Hat der Hersteller in der Risikoanalyse die Risiken aller relevanten Angriffs-Vektoren berücksichtigt und zeigt, wie diese beherrscht werden?
3.	Hat der Hersteller alle Maßnahmen zur Risikobeherrschung auf Wirksamkeit überprüft und diese dokumentiert?

E) Ergänzende Verweise

- MDCG 2020-1 - Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software
  https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2020_1_guidance_clinic_eva_md_software_en.pdf

- MDCG 2019-16 - Guidance on Cybersecurity for medical devices
  https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_cybersecurity_en.pdf

- MDCG 2019-11 - Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR
  https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf

- Bundesamt für Sicherheit in der Informationstechnik – Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/CS-E-132_Medizinprodukte.pdf;jsessionid=B0D46EEE40DFC0FF450C5767154951CC.internet081?__blob=publicationFile&v=1

- OWASP – IoT Security Verification Standard (ISVS)
  https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

- Software Assurance Maturity Model (SAMM)
  https://owaspsamm.org/

- OWASP Top 10 Web Application Security Risks:
  https://owasp.org/www-project-top-ten/
  https://www.owasptopten.org/

- OH KIS: Orientierungshilfe Krankenhausinformationssysteme
  https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html