



Fragebogen

für Hersteller von Medizintechnik
Risikoanalyse nach DIN 80001-1
Risikoanalyse Informationssicherheit

Inhalt

1	Zweck	2
2	Definitionen, Erläuterungen	2
2.1	Definition Medizinprodukte nach Verordnung (EU) 2017/745 über Medizinprodukte	2
2.2	Definition Medizinproduktedurchführungsgesetz (MPDG)	3
2.3	Klassifizierung von Medizinprodukten	3
2.4	Norm IEC 80001-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten.....	5
3.	Abkürzungsverzeichnis.....	6
4.	Ausfüllhinweise	7
5.	Beizulegende Unterlagen	7
6.	Allgemeine Angaben zum Medizinprodukt	8
7.	Kontaktdaten und Ansprechpartner.....	9
8.	Fragen zum Medizinprodukt und seiner Hard-/Software.....	10
8.	Fragen zum Medizinprodukt und seiner Hard-/Software.....	11
8.	Fragen zum Medizinprodukt und seiner Hard-/Software.....	12
8.	Fragen zum Medizinprodukt und seiner Hard-/Software.....	13
8.	Fragen zum Medizinprodukt und seiner Hard-/Software.....	14
9.	Fragen zum Medizinprodukt und seinem Netzwerk	15
9.	Fragen zum Medizinprodukt und seinem Netzwerk	16
10.	Fragen zum Medizinprodukt und Firewall	16
10.	Fragen zum Medizinprodukt und Firewall	17
11.	Fragen zum Medizinprodukt und Updates	17
11.	Fragen zum Medizinprodukt und Updates	18
12.	Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten	19
12.	Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten	20
12.	Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten	21
13.	Fragen zum Medizinprodukt und Fernwartung.....	22

Angaben zum Dokument:

Stand: 20.10.2022
Autoren: Sabine Augustin
Alexander Sparbrod

1 Zweck

Das Universitätsklinikum Jena ist Betreiber einer kritischen Infrastruktur nach § 6 BSI-KritisV und unterliegt damit den gesetzlichen Anforderungen nach § 8a BSIG.

Die Betreuung von Medizinprodukten und medizinischen Gerätschaften zur Diagnostik (zum Beispiel Labordiagnosegeräte) an einem IT-Netzwerk können potenzielle Risiken der Informationssicherheit und Sicherheit der Informationstechnik hervorrufen, die sich wiederum auf die Gesundheit von Patienten, Anwendern oder Dritten auswirken können.

Neben der Patientensicherheit und der Behandlungseffektivität ist ebenfalls die Wahrung der Informationssicherheit bezüglich Verfügbarkeit, Integrität und Vertraulichkeit auch beim Einsatz Medizinprodukten in einem IT-Netzwerk von hoher Bedeutung.

Daher ist es notwendig, möglichst vor Einbindung eines Medizinproduktes an das IT-Netzwerk des UKJ eine interne Risikoanalyse nach DIN 80001-1:2011 und nach ISO/IEC 27001 mit anschließender Maßnahmenbewertung durchzuführen, welche auf Grundlage der Antworten des hier vorliegenden Fragebogens angefertigt wird.

2 Definitionen, Erläuterungen

2.1 Definition Medizinprodukte nach Verordnung (EU) 2017/745 über Medizinprodukte

„Medizinprodukt“ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

- Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
- Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,
- Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben

und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Die folgenden Produkte gelten ebenfalls als Medizinprodukte:

- Produkte zur Empfängnisverhütung oder -förderung,
- Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.

Dazu gehören Implantate, Produkte zur Injektion, Infusion, Transfusion und Dialyse, humanmedizinische Instrumente, Software, Katheter, Herzschrittmacher, Dentalprodukte, Verbandstoffe, Sehhilfen,

Röntgengeräte, Kondome, ärztliche Instrumente, Labordiagnostika, Produkte zur Empfängnisregelung sowie In-vitro-Diagnostika.

Zu den In-vitro-Diagnostika zählen Reagenzien, Reagenzprodukte, Kits, Probenbehältnisse, Geräte und weitere Produkte, die zur In-vitro-Untersuchung von Proben aus dem menschlichen Körper bestimmt sind. Medizinprodukte sind auch Produkte, die einen Stoff oder Zubereitungen aus Stoffen enthalten oder mit solchen beschichtet sind, die bei gesonderter Verwendung als Arzneimittel oder Bestandteil eines Arzneimittels (einschließlich Plasmaderivate) angesehen werden und in Ergänzung zu den Funktionen des Produktes eine Wirkung auf den menschlichen Körper entfalten können.

Anders als bei Arzneimitteln, die pharmakologisch, immunologisch oder metabolisch wirken, wird die bestimmungsgemäße Hauptwirkung bei Medizinprodukten primär auf physikalischem Weg erreicht.

2.2 Definition Medizinproduktedurchführungsgesetz (MPDG)

Das Medizinproduktedurchführungsgesetz (MPDG) dient der Durchführung und Ergänzung der europäischen Medizinprodukteverordnung (EU) 2017/745 (Medical Device Regulation, MDR) und der EU-Verordnung für In-vitro-Diagnostika (EU) 2017/746 (In-vitro Diagnostics Regulation, IVDR). Seit dem 26. Mai 2021 lösen die MDR und das MPDG das Medizinproduktegesetz (MPG) für alle Produkte im Anwendungsbereich der MDR ab. Für In-vitro-Diagnostika ist übergangsweise bis zum Geltungsbeginn der IVDR am 25. Mai 2022 das MPG noch anzuwenden (§ 2 Abs. 1 MPDG). Danach wird der Anwendungsbereich des MPDG auch auf In-vitro-Diagnostika ausgedehnt.

Im Gegensatz zum vorherigen MPG ist das MPDG kein umfassendes Regelwerk, sondern ergänzt die unmittelbar geltenden EU-Medizinprodukteverordnungen (MDR, IVDR) um nationale Vorgaben. Gemeinsam mit dem MPDG regeln die EU-Medizinprodukteverordnungen das Inverkehrbringen und die Inbetriebnahme von Medizinprodukten und sollen dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie der Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritter sorgen.

Außerdem enthält das MPDG spezifische nationale Anforderungen, z. B. zur Durchführung der Überwachung zum Betreiben und Anwenden von Medizinprodukten. Weitere Einzelheiten zum Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten regelt die Medizinprodukte-Betreiberverordnung (MPBetreibV).

2.3 Klassifizierung von Medizinprodukten

Entscheidend für die Klassifizierung sind die Dauer und der Ort der Anwendung eines Medizinproduktes. In der Regel bedeutet dies: je länger das Produkt angewendet wird desto höher ist das Risiko, desto höher die Klassifizierung oder je tiefer das Produkt in den Körper gebracht wird, desto höher das Risiko. Diese Risikoklasse ist für die Zertifizierung entscheidend. Die Klassifizierung wird nach Anhang IX der Richtlinie 93/42/EWG bestimmt. Die Regeln zur Klassifizierung sind detailliert im Anhang VIII der MDR festgelegt.

Der Begriff Klassifizierung ist bei Medizinprodukten mehrfach belegt:

1. Medizinprodukt ja/nein

Die erste Klassifizierung betrifft die Abgrenzung von Medizinprodukten, Nicht-Medizinprodukten und Zubehör zu Medizinprodukten.

2. Klassifizierung I, IIa, IIb, III gemäß MDR¹

Einige Verordnungen definieren selbst wieder Klassen wie die Klassen I, IIa, IIb und III bei der MDR.

Klasse I

Produkte der Klasse I sind meist nicht-invasive Produkte, die keine Auswirkungen auf den menschlichen Körper haben und ein sehr geringes Risiko aufweisen. Klasse I Produkte unterliegen nicht der Zertifizierung durch Benannte Stellen („Notified Bodies“) und können vom Unternehmen selbst zertifiziert werden kann.

Klasse I enthält allerdings drei Unterklassen, für welche Hersteller zum Teil eine Benannte Stelle bei der Konformitätsbewertung einbinden müssen. Medizinprodukte, die in sterilem Zustand auf den Markt gebracht werden, werden als Klasse Is kategorisiert („s“ steht für das englische „sterile“).

Produkte mit Messfunktion werden als Klasse Im bezeichnet („m“ steht für „measure“).

Laut MDR-Gesetz gibt es zudem eine neue Unterklasse: Produkte, die wiederverwendet oder wiederaufbereitet werden können, werden als Klasse Ir („r“ steht für „reusable“) bezeichnet.

Klassifizierung	Definition	Beispiele
Klasse I	Geräte, die nicht steril sind oder keine Messfunktion haben (geringes Risiko)	Rollstühle, Pflaster, Krankenhausbetten, Bettpfannen
Klasse Is	Produkte, die in sterilem Zustand auf den Markt gebracht werden	Schutzausrüstung
Klasse Im	Geräte mit Messfunktion	Stethoskope, Thermometer, Waagen
Klasse Ir	Eine neue Unterklasse für Produkte, die wiederaufbereitet oder wiederverwendet werden	Chirurgische Instrumente und Endoskope

Für Produkte der Klasse I, die keine Zertifizierung durch eine Benannte Stelle erfordern, muss der Hersteller die Dokumente selbst erstellen und vorhalten.

Klasse II

Die nächste Risikoklasse bilden Klasse II-Produkte, die in die Unterklassen IIa und IIb unterteilt sind. Produkte der Klasse IIa bergen ein mittleres Risiko und Produkte der Klasse IIb ein mittleres bis hohes Risiko. Um ein Medizinprodukt der Klasse IIa oder IIb mit der zu versehen und auf den Markt zu bringen, müssen die Hersteller über eine Benannte Stelle verfügen. Diese stellt nach Prüfung der Konformität mit den in der Verordnung festgelegten Verfahren ein CE-Zertifikat aus.

Klassifizierung	Definition	Beispiele
Klasse IIa	Geräte, die kurzfristig (in der Regel 60 Minuten bis 30 Tage) in den Körper eingesetzt werden	Hörgeräte, Ultraschall-Diagnosegeräte, Katheter
Klasse IIb	Geräte, die etwas komplexer als IIa-Geräte sind und oft für mehr als 30 Tage im Körper eingesetzt werden.	Infusionspumpen, chirurgische Laser, Geräte für Intensivüberwachung, Zahnimplantate

¹ (Climedo Health GmbH, 2022)

Klasse III

Produkte mit dem höchsten Risiko für Patienten in die Klasse III eingestuft. Diese Produkte haben entweder lebenserhaltende Funktionen und sind somit von erheblicher Bedeutung für die menschliche Gesundheit oder stellen ein besonders hohes methodisches Krankheits- oder Verletzungsrisiko dar. Um die Sicherheit und Wirksamkeit dieser Produkte zu gewährleisten, ist eine wissenschaftliche Überprüfung vor dem Inverkehrbringen für die Zulassung erforderlich.

Klassifizierung	Definition	Beispiele
Klasse III	Geräte, die unmittelbar am zentralen Kreislauf- oder Nervensystem eingesetzt werden oder ein Medikament enthalten	Herzschrillmacher, prothetische Herzklappe

Digitale Gesundheitsanwendungen

Digitale Gesundheitsanwendungen (kurz "DiGA") sind Medizinprodukte niedriger Risikoklasse (I bis IIa), die dazu bestimmt sein müssen:

- Krankheiten zu erkennen, zu überwachen, zu behandeln oder zu lindern
- Bzw. Verletzungen oder Behinderungen zu erkennen, zu behandeln, zu lindern oder zu kompensieren.

3. Sicherheitsklassen von Software (MDSW) gemäß IEC 62304

Bei Software im Umfeld der Medizinprodukte unterscheidet man

- Software als Teil eines Medizinprodukts, z.B. als embedded Software eines Medizingeräts,
- Software als eigenständiges Medizinprodukt (Standalone-Software),
- Software, die ein Zubehör zu einem Medizinprodukt ist und
- (eigenständige) Software, die kein Medizinprodukt ist.

Unter Software als Medizinprodukt (Software as Medical Device SaMD) versteht man standalone (eigenständige) Software, die ein Medizinprodukt (MP) ist, aber nicht Teil eines solchen.

Unabhängig davon führt die Norm IEC 62304 die Sicherheitsklassen A, B und C ein.

Software, die ein Produkt steuert oder dessen Anwendung beeinflusst, wird derselben Klasse zugerechnet wie das Produkt. Ist die Software von anderen Produkten unabhängig, so wird sie für sich allein klassifiziert. (MDR, Kapitel II, Abs. 3.3)

Die IEC 62304 definiert drei Sicherheitsklassen:

- Klasse A: Keine Verletzung oder Schädigung der Gesundheit ist möglich.
- Klasse B: Keine schwere Verletzung ist möglich.
- Klasse C: Tod oder schwere Verletzung ist möglich.

2.4 Norm IEC 80001-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten

In der medizinischen Praxis werden immer mehr Medizinprodukte in IT-Netzwerke eingebunden. Zunehmend wird Interoperabilität gefordert. Diese Norm definiert Aufgaben, Verantwortlichkeiten und Aktivitäten, damit das Risikomanagement der IT-Netzwerke mit Medizinprodukten die Sicherheit, Effektivität, sowie Daten- und Systemsicherheit eingehalten werden.

3. Abkürzungsverzeichnis

Abkürzung	
UKJ	Universitätsklinikum Jena
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
§ 6 BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) / § 6 Sektor Gesundheit
ISO/IEC 27001	ISO 27001 ist eine internationale Norm für Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen. Sie beschreibt die Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheits-Managementsystems.
IEC 80001-1	Norm zur Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
MP	Medizinprodukt
MPBetreibV	Medizinprodukte-Betreiberverordnung
MDR	Medical Device Regulation europäische Medizinprodukteverordnung
Benannte Stelle	Benannte Stellen sind staatlich „benannte“ (man spricht manchmal auch von „notifizierte“) meist privatwirtschaftliche Unternehmen, die hoheitliche Aufgaben u.a. bei der „Zulassung“ und Überwachung von Medizinprodukten übernehmen.
IVDR	Europäische Verordnung für In-vitro-Diagnostika
MPDG	Medizinprodukte-recht-Durchführungsgesetz
MDSW	Medical Device Software
DiGA	Digitale Gesundheitsanwendung
CE-Kennzeichnung	Medizinprodukte dürfen in Europa und damit auch in Deutschland nur dann in Verkehr gebracht oder in Betrieb genommen werden, wenn sie mit der CE-Kennzeichnung versehen sind. Die CE-Kennzeichnung darf angebracht werden, wenn die Medizinprodukte die Allgemeinen Sicherheits- und Leistungsanforderungen erfüllen und das vorgeschriebene Konformitätsbewertungsverfahren durchgeführt wurde.
UDI-DI	Produktidentifizierungsnummer Unique Device Identification- Device Identifier
UDI-PI	Herstellungskennung - Production Identifier
Active Directory	Active Directory ist also ein zentraler Verzeichnisdienst (engl. directory für Verzeichnis) von Microsoft.
Audit Log	Die Audit-Protokollierung ist der Prozess der Dokumentation von Aktivitäten innerhalb von Softwaresystemen. Prüfprotokolle zeichnen das Auftreten eines Ereignisses, den Zeitpunkt, zu dem es aufgetreten ist, den verantwortlichen Benutzer oder Dienst und die betroffene Einheit auf.
Software-Patch	Ein Software-Patch oder Fix ist eine Schnellreparatur für ein Programm, das Funktionsprobleme behebt, die Sicherheit verbessert oder neue Funktionen hinzufügt.
personenbezogene Daten	All jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben
Data at Rest	Ruhende Daten beziehen sich im Allgemeinen auf Daten, die in einem dauerhaften Speicher (Festplatte, Band) gespeichert sind.
PACS	Ein P icture A rchiving and C ommunication S ystem (PACS, etwa Bildablage- und Kommunikationssystem) ist in der Medizin ein Bildarchivierungs- und Kommunikationssystem auf der Basis digitaler Rechner und Netzwerke
RAID	RAID steht für R edundant A rray of I ndependent D isks, zu Deutsch redundante Anordnung unabhängiger Festplatten. Bei einem RAID-System handelt es sich um einen Verbund mehrerer Festplatten, in dem Daten so gespeichert werden (außer RAID 0), dass sie vor Verlust geschützt sind.
DICOM	D igital I maging and C ommunications in M edicine (DICOM; deutsch: Digitale Bildgebung und -kommunikation in der Medizin) ist ein offener Standard zur Speicherung und zum Austausch von Informationen im medizinischen Bilddatenmanagement.

4. Ausfüllhinweise

Jeder Hersteller eines Medizinproduktes, welches im UKJ an einem Netzwerk betrieben werden soll, ist verpflichtet den Fragebogen verbindlich und vollständig auszufüllen.

Sollten Fragen sachlich nicht relevant sein, so können diese im Bemerkungsfeld als nicht relevant (NR) gekennzeichnet werden.

Es besteht die Möglichkeit mehrere Medizinprodukte einer Produktklasse in einem Fragebogen zusammenzufassen.

5. Beizulegende Unterlagen

Für eine vollumfängliche Risikobewertung und die daraus abzuleitenden Maßnahmen werden nachfolgende Unterlagen benötigt:

- Schematische Darstellung/Übersichtsplan/Netzwerkplan der nachfolgenden aufgeführten Produkte und deren Verbindung
- Schnittstellen/ Verbindungen/ Datenflüsse innerhalb des Systems
- Schnittstellen/ Verbindungen/ Datenflüsse des Systems nach außen
- CE-Kennzeichnung der Produkte, Konformitätserklärung
- Beschreibung der funktionellen Zusammenhänge
- Alle für die Anbindung erforderlichen Schnittstellenbeschreibungen z.B.: DICOM, HL7, usw.
- Conformance Statement (siehe auch Anhang)
- Datenschutzfolgenabschätzung (nur bei der Verarbeitung personenbezogener Daten, die den Kriterien nach Art. 35 DSGVO entsprechen)

6. Allgemeine Angaben zum Medizinprodukt

Nr.	Frage	Antwort Hersteller
6.1	Hersteller inkl. Anschrift	
6.2	Geräteart	
6.3	Typ / Modellbezeichnung einmalige Produktkennung (UDI-DI) Herstellungskennung (UDI-PI)	
6.4	Zweckbestimmung des Medizinprodukts Welche Risikoklasse hat das Medizinprodukt/ medizinische System nach MDR 2017/745?	
6.5	Automatische Inventarisierung	
6.6	Authentifizierung	

7. Kontaktdaten und Ansprechpartner

Nr.	Frage	Antwort Hersteller
7.1	Kontaktdaten des Ansprechpartners für technische Details: Name Telefon E-Mail Geschäftszeiten	
7.2	Kontaktdaten der Verantwortlichen Person nach §15 MDR: Name Telefon E-Mail Geschäftszeiten	
7.3	Kontaktdaten Ansprechpartner seitens des Herstellers für Fragestellungen bzgl. der Vernetzung des Medizinproduktes: Name Telefon E-Mail Geschäftszeiten	
7.4	Kontaktdaten Ansprechpartner seitens des Herstellers im Störfall (ggf. Hotline) Name Telefon E-Mail Geschäftszeiten	

8. Fragen zum Medizinprodukt und seiner Hard-/Software

Nr.	Frage	Antwort Hersteller
8.1	Mit welchem Betriebssystem wird das Gerät bzw. die Software betrieben? Version: Patchstand:	
8.2	Müssen die Komponenten im Rahmen der med. Zweckbestimmung im Netzwerk betrieben werden (Netzwerkzweckbestimmung für das System nach IEC 80001-1)? Wenn ja, warum (Zweck der Einbindung)?	
8.3	Unterstützt das Produkt weitere physische Netzwerkverbindungen?	
8.4	Unterstützt das Produkt kabellose Netzwerkverbindungen? Wenn ja, bitte zählen Sie diese hier auf!	
8.5	Unterstützt das Produkt sichere Übertragungsmethoden oder sind diese implementiert?	
8.6	Benötigt das Produkt eine Internetverbindung? Wenn ja, bitte geben Sie die Mindestanforderung der zur Verfügung stehende Bandbreite an! (Up-/Downloadgeschwindigkeit)	

8. Fragen zum Medizinprodukt und seiner Hard-/Software

Nr.	Frage	Antwort Hersteller
8.7	Handelt es sich um ein gehärtetes Betriebssystem?	
8.8	Verhindert das Produkt einen unautorisierten Zugriff durch eine Nutzeranmeldung oder andere Mechanismen? Wenn ja, welche?	
8.9	Verfügt das Medizinprodukt über ein eigenes Benutzerberechtigungssystem? Gibt es ein zentrales Nutzermanagement? Ist die Anbindung an ein Active Directory möglich?	
8.10	Welche Möglichkeiten der Datensicherung bestehen?	
8.11	Verfügt das Produkt über eine eingebaute Möglichkeit eine Datensicherung auf einem nicht lokalen Speicher durchzuführen? Wenn ja, bitte näher beschreiben!	
8.12	Kann das Produkt personenbezogene Daten mittels dezidierten Kabelanschluss übertragen /empfangen?	

8. Fragen zum Medizinprodukt und seiner Hard-/Software

Nr.	Frage	Antwort Hersteller
8.13	Sind alle Komponenten des Produkts, die private Daten beinhalten physisch abgesichert (d.h. können diese nicht ohne Werkzeug entfernt werden)?	
8.14	Kann der Anwender erkennen, dass keine Datenübertragung stattfindet? Wenn ja, auf welche Art und Weise?	
8.15	Kann der Betreiber die Funktionen des Produkts über ein separates Gerät kontrollieren ?	
8.16	Beschreiben Sie die Auswirkungen auf die Nutzbarkeit des Medizinproduktes bei Ausfall einzelnen Systemkomponenten	
8.17	Gibt es Hinweise bzw. spezielle Risiken betreffend einer Patientengefährdung durch einen IT-Sicherheitsvorfall? Wenn ja, welche und in welchen Dokumenten befinden sich diese Informationen? (Angabe von Dokument und Kapitel, bzw. Seite wo diese Information zu finden ist)	
8.18	Kann das Produkt zusätzlich zu Protokollen des Betriebssystems weitere Audit-Protokolle oder Berichte erzeugen? Wenn ja, welche Protokollierungen werden in Audit Logs vorgenommen und aufgezeichnet?	

8. Fragen zum Medizinprodukt und seiner Hard-/Software

Nr.	Frage	Antwort Hersteller
8.19	Wie sieht der Informationsfluss bzw. die Vorankündigung von: End of Life - / End of Sales -/ End of Support Prozess bei vernetzten Geräten oder vernetzungsrelevanten Komponenten aus?	
8.20	Was passiert bei Ablauf einer regulären Anwendungslizenz? Wird dadurch die Funktion des Produkts beeinträchtigt? oder kann es dadurch zu einer Gefährdung von Patienten kommen?	
8.21	Bitte geben Sie die exakte Bezeichnung der zum Medizinprodukt gehörigen Software an!	
8.22	Bitte geben Sie den Auslieferungszustand der Software-Version des Medizinprodukts an!	
8.23	Wer ist für die Konfiguration und mögliche Datenmigration der Software verantwortlich? (Auftragnehmer / Auftraggeber)	
8.24	Welche Lizenzen für welche Systemteile sind beim Kauf inkludiert? Bitte geben Sie die einzelnen Softwarekomponenten zu den einzelnen Systemteilen an!	

8. Fragen zum Medizinprodukt und seiner Hard-/Software

Nr.	Frage	Antwort Hersteller
8.25	Verfügt die Software über ein eigenes Benutzerberechtigungssystem? Wie kann dieses über ein Active Directory geführt werden?	
8.26	Werden für die eingesetzten Komponenten User- bzw. Herstellerstandardpasswörter verwendet? Müssen die Standardpasswörter geändert werden?	
8.27	Kann das System so konfiguriert werden, dass nach einer bestimmten Zeit der Inaktivität eine neuerliche Anmeldung notwendig wird ?	
8.28	Wie kann der Anwender (bzw. Betreiber) den ordnungsgemäßen Zustand des Systems unter Berücksichtigung der SW-Komponenten überprüfen (vgl. MPBetreibV, Systemhealthcheck)? Werden in diesem Zusammenhang dem Nutzer Systemmeldungen (z.B.: POPUPS) in Klartext bzw. Betriebsmeldungen übersichtlich zur Verfügung gestellt?	

9. Fragen zum Medizinprodukt und seinem Netzwerk

Nr.	Frage	Antwort Hersteller
9.1	Liegt ein Netzwerkplan vor, der beschreibt, wie das Produkt im Netzwerk implementiert ist und wie es kommuniziert? Bitte fügen Sie, wenn vorhanden den Netzwerk und Kommunikationsplan bei!	
9.2	Stellt der Hersteller eine Liste aller Netzwerkports und -protokolle zur Verfügung, die im Produkt genutzt werden oder genutzt werden können? Wenn ja, welche und wofür?	
9.3	Werden Steuerungsmechanismen für den Netzwerkzugriff unterstützt (z.B. interne Firewall oder Whitelisting für Netzwerkverbindungen)? Bitte beschreiben Sie vorhandene Steuerungsmechanismen!	
9.4	Unterstützt das Produkt eine Form der Verbindungsauthentifizierung & Autorisierung (inkl. Zertifikate)? Wenn ja, welche?	
9.5	Welche Maßnahmen bei Netzwerk- oder Datenverlust sind zu treffen?	
9.6	Wie sieht das Procedere aus, wenn das Netzwerk nach einer Unterbrechung wieder zur Verfügung steht?	

9. Fragen zum Medizinprodukt und seinem Netzwerk

Nr.	Frage	Antwort Hersteller
9.7	Welche Risiken in Hinsicht auf Patienten- und Datensicherheit (Schutzziele der DIN EN 80001) ergeben sich durch die Vernetzung bei Gebrauch?	

10. Fragen zum Medizinprodukt und Firewall

Nr.	Frage	Antwort Hersteller
10.1	Kann ein Host-basiertes System zur Erkennung oder Abwehr von Angriffen konfiguriert oder installiert werden? Wenn ja, welches?	
10.2	Unterstützt das Produkt die Verwendung von Anti-Schadsoftware oder anderen Mechanismen zur Abwehr von Schadprogrammen? Wenn ja, gibt es Herstellervorgaben? Ist etwas vorinstalliert? Wie ist das Vorgehen bei Aktualisierung der Software?	
10.3	Wenn keine Anti-Schadsoftware auf dem Produkt installiert werden kann, sind andere Schutzmechanismen implementiert oder verfügbar?	

10. Fragen zum Medizinprodukt und Firewall

Nr.	Frage	Antwort Hersteller
10.4	Gibt es einen Prozess des Herstellers für die regelmäßige Überprüfung auf Schwachstellen für die angebotenen Systeme? Wie wird der Anwender informiert? Wird ein Maßnahmenkatalog zur Verfügung gestellt?	

11. Fragen zum Medizinprodukt und Updates

Nr.	Frage	Antwort Hersteller
11.1	Läuft auf dem Produkt irgendwelche Software oder Firmware (damit ist sowohl vom Hersteller selbst als auch durch Drittanbieter hergestellte Software gemeint), die Sicherheits-Updates während ihrer geplanten Verwendungszeit benötigt?	
11.2	Informiert der Hersteller den Kunden, wenn Updates zur Installation freigegeben worden sind oder kann das Produkt automatisch Software Updates installieren? Wenn ja, bitte näher beschreiben!	
11.3	Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software Patches oder Updates für diese Merkmale durchzuführen?	

11. Fragen zum Medizinprodukt und Updates

Nr.	Frage	Antwort Hersteller
11.4	Ist es erlaubt, dass Sicherheits-Updates für diese Merkmale oder das Produkt selbst durch Dritt-Komponenten-Anbieter ohne vorherige Freigabe des Herstellers installiert werden?	
11.5	Ist es möglich Software Patches und Updates für diese Merkmale auf dem Produkt per Fernwartung zu installieren?	
11.6	Existiert eine Anzeige oder Meldung für einen freigeschalteten und aktiven Fernwartungszugriff?	
11.7	Verfügt der Hersteller über einen Prozess, um Schwachstellen und Updates zu bewerten?	
11.8	Wird ein Internet-Proxy unterstützt?	

12. Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten

Nr.	Frage	Antwort Hersteller
12.1	Kann das Gerät personenbezogene Daten anzeigen, übertragen, speichern oder verändern (inkl. elektronischer Akten)?	
12.2	Werden personenbezogene Daten in einer Datenbank, auf dem Produkt selbst oder außerhalb des Produkts gespeichert?	
12.3	Werden im Produkt oder der Software personenbezogene Daten temporär oder in einem flüchtigen internen Speicher vorgehalten ?	
12.4	Hat das System einen (primären) Langzeitspeicher von personenbezogenen Daten oder andere Patientendaten ?	
12.5	Bietet das Produkt Fehlersicherungsfunktionen und Wiederherstellungsmechanismen für gespeicherte Gesundheitsdaten ?	
12.6	Speichert oder verwaltet das Produkt oder die Anwendung selbst die Anmeldedaten für Personen Wenn ja, bitte beschreiben Sie die Implementierung!	

12. Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten

Nr.	Frage	Antwort Hersteller
12.7	Können personenbezogene Daten von anderen Systemen importiert oder dorthin exportiert werden? Wenn ja, über welche Schnittstellen können diese Übertragungen stattfinden?	
12.8	Ist eine Datenverschlüsselung mit dem Produkt möglich bzw. kann das Produkt abgelegte Daten verschlüsseln? Werden personenbezogene Daten verschlüsselt, bevor sie durch ein Netzwerk übertragen oder auf einen Wechseldatenträger kopiert werden? Wenn ja, bitte geben Sie den Verschlüsselungsmechanismus an!	
12.9	Unterstützt das Produkt eine Anonymisierung von Profilen nach DICOM Standard? Wenn ja, bitte beschreiben Sie dies näher!	
12.10	Verfügt das Produkt über einen eingebauten Mechanismus, um personenbezogene Daten zu de-identifizieren?	
12.11	Verfügt das Produkt über Mechanismen zur Prüfung der Integrität gespeicherter Gesundheitsdaten ?	

12. Fragen zum Medizinprodukt – Verarbeitung personenbezogener Daten

Nr.	Frage	Antwort Hersteller
12.12	Wie können lokale Patientendaten bei Austausch oder Stilllegung des Medizinproduktes am Medizingerät wieder exportiert bzw. einfach und sicher gelöscht und vernichtet werden?	
12.13	Werden Neuentwicklungen abwärtskompatibel ausgeführt im Sinne der Lesbarkeit und korrekten Darstellung bzw. Wiedergabe von Altdaten?	
12.14	Werden die vom Medizinprodukt erhobenen Daten in einer Cloud gespeichert oder verarbeitet? Wenn ja, bitte geben Sie den Cloudanbieter an!	

13. Fragen zum Medizinprodukt und Fernwartung

Nr.	Frage	Antwort Hersteller
13.1	Ist eine Fernwartung möglich? Wenn ja: ist diese verpflichtend?	
13.2	Wie wird der Fernwartungszugang gesichert? Bitte geben Sie hier sowohl technische als auch prozessorientierte Informationen an!	
13.3	Gibt es Regelungen seitens des Herstellers für zugriffsberechtigte Personen bei einer Fernwartung? Wenn ja, bitte beschreiben Sie das Zugriffskonzept!	
13.4	Wird VPN-Technologie unterstützt?	

Hinweis: Um ausgefüllte Formularfelder vor nachträglicher Veränderung zu schützen, drucken Sie dieses Formular als PDF-Datei aus und speichern es unter einem anderem Namen ab