Questionnaire "Cybersecurity for Medical Devices - Technical Documentation"

Version 1, dated 21st of March, 2023

1. Preliminary remarks

- This document was compiled by the German Notified Bodies Alliance ("Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland", IG-NB) and is intended to serve as orientation for Notified Bodies, manufacturers and interested parties. It makes no claim to completeness or mandatory application.
- This document covers assessments of Technical Documentation for MDR / IVDR. Not all requirements of MDR, IVDR and MDCG 2019-16 are covered in this document.
- Created by Jan Küfner (TÜV SÜD), Dr. Abtin Rad (TÜV SÜD), Dr. Andreas Schwab (TÜV Rheinland), Volker Sudmann (mdc medical device certification), Markus Bianchi (DNV Medcert), Martin Tettke (Berlin Cert), Michael Bothe (DQS Med), Mark Küller (TÜV-Verband / IG-NB). It replaces the previous version "IT Security for Medical Devices" (Version 5, 09.06.2022).
- Questions regarding the security risks of artificial intelligence can be found in latest version of IG-NB's "Questionnaire Artificial Intelligence (AI) in Medical Devices".
- Compliance to IEC 81001-5-1 is not expected, however recommended, prior to the end of its transition period. Compliance to IEC 81001-5-1 prior its transition period is however recommended. In the following tables IEC 81001-5-1 is mentioned only for complementary purposes. Questions for manufacturers are solely based on the current requirements (MDR, IVDR, MDCG 2019-16)
- Since cybersecurity evolves on a regulatory and technological level, this document is intended to reflect the current state of the art at the time of creation only.

References:

- Regulation (EU) 2017/745 (MDR), dated 5 April 2017
- MDCG 2019-16 - Guidance on Cybersecurity for medical devices, Rev. 1, 2020-07
- IEC 62304:2006-05 Medical device software - Software life cycle processes
- IEC 81001-5-1:2021-12 Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

2. System Description

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
2.1	State of the Art (SOTA)	An appropriate system diagram must be available.	Is an appropriate system diagram available?	Yes, see:- Software development plan- Software architecture

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
2.2	IEC 81001-5-1 cl. 7.2	'All products have a threat model specific to the current development scope. Characteristics (where applicable): correct flow of categorized information throughout the system, trust boundaries, data stores, internal/external communication protocols etc.'	Note: a complete system diagram should include the following:1. All medical devices incl. their interfaces (e.g. bluetooth, wifi, ethernet), utilized protocols (e.g. HL7, DICOM, HTTPS, MQTTS, custom) on those interfaces and their implemented technical specification (e.g. implemented protocol version) incl. the type of data being transferred (e.g. personal health information, therapeutic commands, updates, remote access) on those interfaces.2. All human machine interfaces within the system (e.g. screens, keyboards).	Potential cyber security risks and IT-security concerns have been taken into account within the framework of the existing FMEA risk analysis, following the ISO 14971 standard for risk management in medical devices.

3. Security Risk Management

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.1	MDCG 2019-16 cpt. 3.2	'The security risk management process has the same elements as the safety risk management process, all documented in a security risk management plan. The process elements are security risk analysis, security risk evaluation, security risk control, evaluation of residual security risk and reporting.'	Is a security risk analysis available?	Yes, see:- Risk management plan- Risk table- Risk management report

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.2	MDCG 2019-16 cpt. 3.4and IEC 81001-5-1 cl. 7.2	‘Threat Modelling techniques are a systematic approach for analyzing the security of an item in a structural way such that vulnerabilities can be identified, enumerated and prioritized, all from a hypothetical attacker’s point of view.’AND‘(. . .) Employ activities to ensure that all products have a threat model specific to the current development scope.’	Does the security risk assessment contain an appropriate and systematic threat model?Note: STRIDE is a systematic threat modelling technique, since it evaluates threat categories interface by interface.	Potential cyber security risks and IT-security concerns have been taken into account within the framework of the existing FMEA risk analysis, following the ISO 14971 standard for risk management in medical devices.

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.3	MDCG 2019-16 cpt. 3.4	'Threat modelling typically employs a systematic approach to identify attack vectors and assets most desired by an attacker.'AND-'Establish activities which identify and document any vulnerabilities, threats and associated adverse impacts affecting confidentiality, integrity, availability of assets.-Consider intended use and the intended environment of use.'	Is the threat model complete and correct (e.g. discussing all applicable threats for all relevant attack vectors)?	Yes, see risk table.

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.4	IEC 81001-5-1 cl. 7.3	- Establish activities to estimate risk of vulnerabilities.-Risk estimation should consider adverse impact of vulnerability to security-Estimation can be supported by using vulnerability scoring-Scoring system can be based on a likelihood/severity scheme used by the manufacturer for other risks-Evaluate estimated risks-Determine if risk is acceptable or not (based on scoring)-Inform product risk management process	Is the risk pre- and post-mitigation appropriately esti-mated?Note 1: quantitative risk assessment is accept-able.Note 2: security risk is a combination of exploitability and severity.Note 3: alteration or disclosure of patient data can lead to harm.	Yes, see:- Risk table- Risk management report

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.5	MDCG 2019-16 cpt. 3.2	'When a security risk or control measure could have a possible impact on safety and effectiveness, then it should be included in the safety risk assessment.'	Are security mitigations (if any) that might affect safety appropriately discussed?	Yes, see:- Risk table- Risk management report

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.6	MDCG 2019-16 cpt. 3.3	'Where there is an impact on safety or effectiveness, manufacturers shall select the most appropriate risk control solution, in the following order of priority:a) Eliminate or reduce risks as far as possible through safe design and manufacture;b) Where appropriate, take adequate protection measures, including alarms if necessary, in relation to risks that cannot be eliminated;c) Provide information for safety (warnings/precautions/contraindications) and, where appropriate, training to users.For security, a similar approach can be taken:a) Eliminate or	Do risk control solutions have the correct order or priority?Note: according to MDR/IVDR, the auditee shall always implement security measures within the device rather than delegating security via IFU to the user or admin of the device.	Yes, see:- Risk table- Risk management report

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.7	IEC 81001-5-1 cl. 7.4	- Determine whether security risk control measures are appropriate for reducing security risks to an acceptable level (based on security risk acceptance policies)- If risk controls are deemed appropriate: appropriate mitigations selected- Determine whether mitigations result in new risks or increased other risks,- Select mitigations implemented, effectiveness of the implemented measures verified	Are risk control measures / counter measures appropriate?	Yes, see:- Risk table- Risk management report

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
3.8	MDCG 2019-16 cpt. 2.1and- MDR Annex I (17.4) / IVDR Annex I (16.4)and- MDR Annex I (18.8)and- MDR Annex I (17.2) / IVDR Annex I (16.2)	‘Key concepts involved in IT security specifically for medical devices are the following:- Confidentiality of information at rest and in transit- Integrity, which is necessary to ensure information authenticity and accuracy (i.e. non-repudiation)- Availability of the processes, devices, data, and connected systems.‘AND‘Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.’AND‘Devices shall be	Is the security concept of the device under evaluation appropriate?	Yes, see:- Risk table- Risk management report- Software development plan

4. Accompanying Documentation

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
4.1	MDCG 2019-16 cpt. 2.6and-MDR Annex I (23.4.ab) / IVDR Annex I (20.4.1.ab)	'While the MDR and the IVDR provide legal obligations only with regard to manufacturers, however it should be noted that for the provision of secured healthcare services, it is important to recognize the roles and expectations of all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators. All of these actors share responsibilities for ensuring a secured environment for the benefit of patients' safety.'ANDThe instructions for use shall contain all of the following particulars:	Are the responsibilities of manufacturer, integrator and users correctly reflected in the IFU?Note: in cases where the medical device relies on the operating environment to provide essential IT security controls, this is appropriately stated in the accompanying technical documentation.	Yes, see:- Instructions for use / user manual

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
4.2	MDCG 2019-16 cpt. 4.2	'The requirements regarding the instructions for use are outlined in the following articles of Annex I'	Does the accompanying documentation appropriately contain the following (if applicable):- Any residual cybersecurity risk communicated as limitation, contraindication, precaution or warning- Information about product installation such as configuration of security features (CNFS). Note: this does NOT mean the documentation /or provisioning of passwords for assessment in the accompanying documents. Also include required information about any necessary 3rd party software such as anti-virus software, firewall, malware 15 detection/protection (MLDP) and minimum requirements for OS, workstation,	Yes, see:- Instructions for use / user manual- User training

5. Lifecycle (Relevant Output Documents)

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
5.1	IEC 62304 cl. 8.1.2	'Document for each SOUP configuration item being used (incl. standard libraries): title, manufacturer, unique SOUP designator."	Has the manufacturer documented all SOUP components?	Yes, see:- SOUP

Item	Source	Requirement(s)	IG-NB Commentary	Manufacturer Reference for Compliance
5.2	MDCG 2019-16 cpt. 3.7 and IEC 81001-5-1 cl. 5.7.5	'The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing.' AND 'Documented means of ensuring objectivity of the test effort for security requirements testing, known vulnerability scanning and penetration testing.'	- Is the penetration test report available and appropriate?- Is the penetration test covering all applicable attack vectors?- Is the tester appropriately skilled?- Is the tester independent?- Are appropriate tools used?- Is enough time / resources utilized? Is appropriate Fuzz Testing conducted where applicable?Note 1: Common penetration testing methodologies such as open-source security testing methodologies (OSSTMM), MASTG, phased structured approaches such as penetration testing execution standard (PTES) methodologies should be adapted as appropriate for the	Security verification and validation was performed as part of system testing. See system test results.