Questionnaire “Cybersecurity for Medical Devices - Technical Documentation”

(Version 1, 21.03.2023)

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.
- This document is covering Technical Documentation Assessments (TDA) for MDR / IVDR.
- 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)
- This document, together with the questionnaire “Cybersecurity for Medical Devices – Audit“, replaces the questionnaire "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" (https://www.ig-nb.de/veroeffentlichungen).
- Not all requirements of MDR, IVDR and MDCG 2019-16 are covered in this document. Compliance to IEC 81001-5-1 is not expected prior 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.

- There are few cybersecurity experts today and it is likely that the situation will continue to be similar in the foreseeable future; therefore it is one goal of this paper to help making conformity assessment(s) of cybersecurity as efficient as possible without compromising the quality.
- The terminology used in this document is derived from the terms and definitions within the referenced sources. E.g. cybersecurity as defined in ISO 81001-1:2021-12, cl. 3.30.
- Included in this document are references to paragraphs from the standards IEC 62034 and IEC 81001-5-1. These standards have different scopes (medical device software (IEC 62304) and healthcare software (IEC 81001-5-1)) and use different terms for similar subjects and processes. Specific terms and their use in the context of the respective standard are defined in clause 3 "Terms and Definitions" of the respective standard.
- The document makes no claim to completeness or mandatory application.

References

- REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (2017/745/EU) (MDR)
- REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (2017/746/EU) (IVDR)
- 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

Terms and Definitions

- In this document, the term medical device is frequently used. Whenever the term medical device is mentioned, both types are meant, medical devices and in vitro diagnostic medical devices.

Changes to last version

/

1 System Description

	Source	Requirements	Questions / Comments
1.	State of the Art (SOTA)	An appropriate system diagram must be available.	Is an appropriate system diagram available? Note: A complete system diagram is an essential part of the threat model and should to include the following: • All medical / IVD devices & non-medical devices o incl. their interfaces (e.g. Bluetooth, Wi-Fi, Ethernet) o incl. protocols utilized (e.g. HL7, DICOM, HTTPS, MQTTS, custom) on those interfaces and their implemented technical specification (e.g. implemented protocol version) o incl. the type of data being transferred (e.g. personal health information (PHI), therapeutic commands, updates, remote access) on those interfaces. • All human machine interfaces (e.g. screens, keyboards) within the system
2.	IEC 81001-5-1 cl. 7.2	– all products have a threat model specific to current development scope – characteristics (where applicable): correct flow of categorized information throughout system, trust boundaries, data stores, internal/ external communication protocols implemented, headers which might be used to attack the hardware, …	

2 Security Risk Management

	Source	Requirements	Questions / Comments
1.	MDCG 2019-16 chapter 3.2	‘The security risk management process has the same elements as 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?
2.	MDCG 2019-16 chapter 3.4	‘Threat Modelling techniques are a systematic approach for analysing the security of an item in a structural way such that vulnerabilities can be identified, enumerated, and prioritised, all from a hypothetical attacker’s point of view.’	Does the security risk assessment contain an appropriate and systematic threat model? Note: STRIDE is a systematic threat modelling technique, since it evaluates thread categories interface by interface.
	IEC 81001-5-1 cl. 7.2	– employ activities to ensure that all products have a threat model specific to the current development scope	
3.	MDCG 2019-16 chapter 3.4	‘Threat modelling typically employs a systematic approach to identify attack vectors and assets most desired by an attacker.’	Is the threat model complete (e.g. discussing all applicable threats for all relevant attack vectors) and correct?
	IEC 81001-5-1 cl. 7.2	– 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	
4.	IEC 81001-5-1 cl. 7.3	– establish activities to estimate risk of vulnerabilities	Is the risk pre- and post-mitigation appropriately estimated?

	Source	Requirements	Questions / Comments
		– 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	Note 1: Quantitative risk assessment is acceptable. Note 2: Security risk is a combination of exploitability and severity. Note: Alteration or disclosure of patient data can lead to harm
5.	MDCG 2019-16 chapter 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?
6.	MDCG 2019-16 chapter 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; b) Where appropriate, take adequate protection measures, including security notifications if necessary, in relation to risks that cannot be eliminated; c) Provide information for security (warnings/precautions/contra-indications) including information on measures that the user is required to take in the operating environment to reduce the likelihood of exploitation.	Do risk control solutions have the correct order of priority? Note: According 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.

	Source	Requirements	Questions / Comments
		c) Provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users. For security, a similar approach can be taken: a) Eliminate or reduce security risks as far as feasible through secure design and manufacture;’	
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?
8.	MDCG 2019-16 chapter 2.1	‘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‘	Is the security concept of the device under evaluation appropriate?
	MDR Annex I (17.4) IVDR Annex I (16.4)	‘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.’	

	Source	Requirements	Questions / Comments
	MDR Annex I (18.8)	‘Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended.’	
	MDR Annex I (17.2) IVDR Annex I (16.2)	The Cybersecurity risks are as far as possible reduced without adversely affecting the benefit-risk ratio. The device is developed in accordance with the state of the art taking into account the principles of risk management, including information security.	

3 Accompanying Documentation

	Source	Requirements	Questions / Comments
1.	MDCG 2019-16 chapter 2.6	'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.'	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.
	MDR Annex I (23.4. ab) IVDR Annex I (20.4.1 ah)	The instructions for use shall contain all of the following particulars: 'for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, minimum requirements concerning hardware, IT networks characteristics and **IT security measures, including protection against unauthorised access, necessary to run the software as intended**.'	

	Source	Requirements	Questions / Comments
2.	MDCG 2019-16 chapter 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 o configuration of security features (CNFS) o Note: This does NOT mean the documentation /or provisioning of passwords for assessment in the accompanying documents. o required information about any necessary 3rd party software such as anti-virus software, firewall, malware detection/protection (MLDP) o minimum requirements for OS, workstation, peripherals • procedures for using the medical device in fail-safe mode / action plan for users to follow in case of alert messages • information about user requirements in terms of training / required skills • instruction on installing (cybersecurity) updates & patches (CSUP) • the environment of use (home environment, healthcare facility, etc.) • a description of data backup (DTBK) and restore features • user roles incl. privileges • information about logging

4 (relevant output documents of the) Lifecycle

	Source	Requirements	Questions / Comments
1.	IEC 62304 cl. 8.1.2	– document for each SOUP configuration item being used (including standard libraries): title, manufacturer, unique SOUP designator	Has the manufacturer documented all SOUP components?
2.	MDCG 2019-16 chapter 3.7	'The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing.'	• Is the penetration test report available and appropriate? o Is the penetration test covering all applicable attack vectors? o Is the tester appropriately skilled? o Is the tester independent? o Are appropriate tools used? o 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 medical device until appropriate standards are available. Note 2: The penetration test should consider any special constraints relating to the medical device(s) such as the safety of the patient and others as well as clinical performance.
	IEC 81001-5-1 cl. 5.7.5	– documented means of ensuring objectivity of the test effort for security requirements testing, known vulnerability scanning and penetration testing	

	Source	Requirements	Questions / Comments
			Note 3: ISO 17025 accredited test laboratories with appropriate capability and competence for medical device penetration testing should be used once available.