IG-NB
Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland

Questionnaire "IT Security for Medical Devices“

(Version 5, 09.06.2022)

Preliminary remarks:

- This questionnaire 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 third parties.
- This document raises key issues in the assessment of IT security of medical devices and provides references to the essential laws and standards. The document is to be revised regularly and adapted to the current status of standards.
- The document makes no claim to completeness or mandatory application.
- The focus of the assessment results from the intended use.
- This questionnaire is based in part on the „IT Security Guideline for Medical Devices“ by TÜV SÜD, Johner Institute and Dr. Georg Heidenreich (https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_EN.md).
- Questions regarding the security risks of artificial intelligence can be found in IG-NB's "Questionnaire Artificial Intelligence (AI) in Medical Devices".

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)
- 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)
- COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices (93/42/EEC)
- EN ISO 13485:2016-08 Medical devices - Quality management systems - Requirements for regulatory purposes
- EN ISO 14971:2013-04 Medical devices - Application of risk management to medical devices
- IEC EN 60601-1:2013-12 Medical electrical equipment - Part 1: General requirements for basic safety and essential performance
- IEC EN 62304:2016-10 Medical device software - Software life-cycle processes
- IEC EN 62366:2008-09 Medical devices - Application of usability engineering to medical devices
- ISO/TR 80002-2:2017-06 Medical device software - Part 2: Validation of software for medical device quality systems (ISO TR 80002-2)
- IEC EN 82304-1:2018-04 Health Software – Part 1: General requirements for product safety

Main changes to Version 4:

> Translation German / English

> Adjustments/corrections in: B 2 A 1

Table of contents:

A) General requirements

1. Competences

1.	Does the manufacturer have adequate records of education, training and competences to conclude that people actually have these competences (with regard to cyber-security)? How does the organisation present competence requirements with regard to IT security?	• ISO 13485, 6.2. • ISO 14971, 3.3.
2.	Is the involvement of external competences in accordance with the requirements of outsourced processes? How is the competence of outsourced persons recorded/documented?	• ISO 13485, 4.1.5., 7.3.2.

2. Documentation

1.	Has the manufacturer documented compliance with the cyber security requirements as part of the general safety and performance requirements?	• 2017/745/EU, Annex I, 17.2., 17.4. • 2017/746/EU, Annex I, 16.2., 16.4. • (93/42/EEC, Art. 3) • ISO 13485, 7.3.6., 7.3.7.

B) Process requirements

1. Requirements for the product development

a) Intended use and stakeholder requirements

1.	Has the manufacturer determined all neighbouring systems (medical devices, IT systems) that can be connected to the device?	• 2017/745/EU, Annex I, 14.1., 14.2. (d) • 2017/746/EU, Annex I, 13.1., 13.2. (d) • (93/42/EEC, Annex I, 9.1., 13.6. (c)) • IEC 82304-1, 4.1. (b), 4.2. (d)
2.	Has the manufacturer determined the intended environment of use (hardware and software)?	• IEC 60601-1, 14.13. • IEC 62304, 5.2.2. • IEC 82304-1, 4.1., 4.2.
3.	Has the manufacturer analysed the risks / hazards (with regard to the specified users) and the environment? How is unauthorised access prevented? How is use in a non-specified environment prevented?	• 2017/745/EU, Annex I, 14.2. (d) • 2017/746/EU, Annex I, 13.2. (d) • IEC 82304-1, 4.1. (c)
4.	Has the manufacturer described, in the context of risk management, which threats to IT security exist and which hazards for patients, users and third parties arise from this?	• IEC 62304, 7.1.2.
5.	Has the manufacturer examined each usage scenario and what risks arise from unspecified display of information (e.g. no display, wrong display, too late display)?	• IEC 62366-1, 5.3., 5.4.
6.	Has the manufacturer specified the protocols and standards used for each data interface?	• IEC 62304, 5.2.2. • IEC 82304-1, 4.2. (b)

b) System and software requirements

i) Authentication and authorisation

1.	Has the manufacturer justified the appropriateness of the authentication procedure (user name/password, biometric procedure, token (e.g. card) etc.) for all roles and all neighbouring systems?	• ISO 14971, 6.6.
2.	Has the manufacturer analysed within the risk management the implications for patient safety if a person cannot access patient or device data (e.g. no authorisation, forgotten password) and defined appropriate measures?	• ISO 14971, 6.6.

ii) Data, communication

1.	Has the manufacturer identified all data managed by the system?	• IEC 62304, 5.5.2. (b), 5.5.2. (e)
2.	Has the manufacturer assessed how important protection of data is in relation to confidentiality and its impact on patient safety?	• IEC 62304, 7.1.2.
3.	Has the manufacturer assessed, in the context of risk management, the consequences if the protection of data requiring special protection is no longer given?	• IEC 62304, 7.1.2.
4.	Has the manufacturer examined, in the context of risk management, the consequences of system overload due to too many requests (e.g. DoS (Denial of Service)) or requests with too large data volumes and, if necessary, defined actions?	• 2017/745/EU, Annex I, 14.2. (d), 17.2. • 2017/746/EU, Annex I, 13.2. (d), 16. • IEC 82304-1, 4.2.10., 4.5. (e)
5.	Has the manufacturer analysed, in the context of risk management, the consequences if the network is no longer available or no longer available in the expected quality?	• 2017/745/EU, Annex I, 17.4. • 2017/746/EU, Annex I, 16.4. • IEC 60601-1, 14.13.
6.	Has the manufacturer analysed, in the context of risk management, the consequences of the loss of data and defined actions if necessary (e.g. backup and recovery of data)?	• IEC 60601-1, 4.3.
7.	How does the manufacturer ensure that external data are checked for validity before processing?	• 2017/745/EU, Annex I, 14.1., 14.2. (d), 18.8. • 2017/746/EU, Annex I, 13.1., 13.2. (d)

iii) Patches

1.	Has the manufacturer established a deployment process for updates, patches, etc.? Does this include the question of who is allowed to apply patches?	• IEC 62304, 6.
2.	How is the interface to vigilance defined?	• IEC 62304, 6.1. (b)
3.	Does the manufacturer has a list of all SOUP/OTS components?	• IEC 62304, 8.1.2.

iv) Other

1.	What measures have been implemented to detect attacks on IT security or the compromise of IT security?	• IEC 62304, 5.2.3., 5.2.4. • IEC 82304-1, 4.5. (f)
2.	Has the manufacturer assessed which functionality the medical device must provide even in the event of a compromise of IT security (essential performance features)?	• IEC 60601-1, 4.3. • IEC 82304-1, 4.5. (g)

c) System and software architecture

1.	Has the manufacturer documented all SOUP/OTS components (incl. version, manufacturer, reference to information on updates, release notes)?	• IEC 62304., 8.1.2
2.	Has the manufacturer analysed the specific risks arising from the choice of technologies (especially programming language, SOUP/OTS components including operating systems)? Does it update this analysis on an ongoing basis? Have platform-specific factors (e.g. storage leaks C++, Android, ...) been considered? How does the manufacturer keep up to date regarding these specific risks?	• ISO 13485., 8.3 • IEC 62304, 5.3.3., 5.1.7., 7.1.3., 8.1.2. • IEC 82304-1, 4.7., 8.2.
3.	Has the manufacturer taken measures to ensure that the tools used (e.g. development environment, compiler), as well as the platforms and SOUP/OTS components are free of malicious code?	• ISO 13485, 4.1.6., 7.5.6. • ISO TR 80002-2
4.	Has the manufacturer created a list of all services that the product offers or uses (e.g. through its operating system) to the "outside world"?	• 2017/745/EU, Annex I, 4. (a) • 2017/746/EU, Annex I, 4. (a) • (93/42/EEC, Annex I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.

5.	Has the manufacturer justified for each service why it must be visible externally (for an unlimited period of time)?	• 2017/745/EU, Annex I, 4. (a) • 2017/746/EU, Annex I, 4. (a) • (93/42/EEC, Annex I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.
6.	If the product offers an interface, has the manufacturer described in the context of risk management how attacks via this interface are controlled?	• 2017/745/EU, Annex I, 4. (a) • 2017/746/EU, Annex I, 4. (a) • (93/42/EEC, Annex I, 2.) • IEC 60601-1, 14.13. • IEC 82304-1, 7.2.3.
7.	Has the manufacturer determined for each role and each neighbouring system the functions of the product that it is allowed to access via the respective interface?	• IEC 82304-1, 7.2.3.2. (c)
8.	For each externally visible service, has the manufacturer identified the process that provides / implements this service?	• IEC 62304, 5.3.
9.	Has the manufacturer determined how the product detects a compromise of IT security, documents it (log-file) and how it reacts to it?	• IEC 82304-1, 4.5. (f)
10.	Has the manufacturer analysed for all software components, services or processes, data and software components what risks arise if they do not behave in accordance with the specifications due to a problem with IT security?	• IEC 60601-1, 14.13. • IEC 62304, 7.1.2. • IEC 82304-1, 7.2.3.2.
11.	Has the manufacturer taken the software requirements into account in the software architecture? Are security-relevant requirements taken into account in the software architecture?	• IEC 62304, 5.3.1.

d) Implementation and development of the software

1.	Has the manufacturer created coding guidelines that set requirements specific to IT security?	• IEC 62304, 5.1., 5.5.3.
2.	Has the manufacturer either proofed the software (source code and binaries) for malicious code before delivery and/or protected all computers involved in the development and "production" of the software against malware (integrity of the distribution channel)?	• IEC 62304, 5.8.8.

	How is it ensured that installation packages are not illegally modified before installation (integrity of the distribution channel, e.g. through checksums, signing, ...)?	

e) Evaluation of software units

1.	How does the manufacturer ensure that IT security has been taken into account in the development of the software units (security-by-design)?	• IEC 62304, 5.1.1., 5.5.3.

f) System and software tests

1.	Has the manufacturer documented an adequate description of the selection and appropriateness of tests regarding compliance with the requirements of the cyber security measures defined in the risk management that confirm the effectiveness of the control measures?	• ISO 14971, 6.2., 6.3.
2.	Has the manufacturer made provisions for the testing of all system/software requirements in the test plan?	• IEC 62304, 5.1.1. (c), 5.1.6.

g) Product release

1.	Has the manufacturer prepared the necessary plans for the post-development phase regarding IT security (e.g. post-market and incident response plan, incl. SOUP)?	• 2017/745/EU, Chapter VII • 2017/746/EU, Chapter VII • ISO 13485, 8.2.1., 8.2.2. • IEC 62304, 6, 7.1.3.
2.	Has the manufacturer checked the completeness of the tests and linked the tests to the requirements?	• IEC 62304, 5.8.1, 5.8.6. • IEC 82304-1, 6.

2. Requirements for the post-development phase

a) Production, distribution, installation

1.	Has the manufacturer described how it is ensured that only exactly the intended artefacts (files) are delivered in exactly the intended version in the product or as a product?	• IEC 62304, 5.8.8.
2.	Has the manufacturer described how the persons responsible for the installation can obtain the knowledge of which is the latest version and how confusion during installation can be excluded?	• ISO 13485, 7.8.3., 8.3. • IEC 62304, 5.8.4.

3.	Has the manufacturer described how it will be ensured during installation that the requirements specified in the accompanying materials are actually met?	• ISO 13485, 7.5.3.
4.	Has the manufacturer established procedures to ensure that it is able to communicate with the operators and users of its products in a timely manner?	• ISO 13485, 7.2.3., 8.3.3. • IEC 82304-1, 8.4.
5.	Has the manufacturer specified and communicated minimum requirements regarding hardware, IT network characteristics and IT security measures, including protection against unauthorised access?	• 2017/745/EU, Annex I, 17.4. • 2017/746/EU, Annex 1, 16.4.

b) Post-market surveillance

1.	Has the manufacturer prepared a post-market surveillance plan that also adequately addresses IT security issues? - Has the manufacturer described what information is collected from the post-production phase, in particular on additional attempted or successful compromise? - Has the manufacturer described how and through which channels information from the post-production phase is collected? - Has the manufacturer described how information from the post-production phase is analysed and evaluated? - Has the manufacturer described what measures result from this? - For each SOUP/OTS component, has the manufacturer defined at least one source and the frequency of its monitoring, through which it is informed of IT security-related problems? Has it described which role performs this evaluation and with which tools? - Has the manufacturer described how it monitors that used technologies and procedures (e.g. cryptography) are still secure?	• 2017/745/EU, Chapter VII • 2017/746/EU, Chapter VII • (93/42/EEC, Art. 10)

c) Incident Response Plan

1.	Is the manufacturer's IT security incident handling capable of responding to emergencies within the shortest possible time?	• 2017/745/EU, Art. 87 • 2017/746/EU, Art. 82 • (93/42/EEC, Art. 10) • IEC 82304-1, 8.4.

d) Decommissioning

1.	Is there a lifecycle concept for patient data (which includes protection against unintentional deletion as well as change of use and final deletion)?	• IEC 82304-1, 8.5.

C) Product requirements

Preliminary remark:
The following are questions about a possible implementation. References to legislation and standards have been omitted, as the questions result from the processes requirements (Chapter B).

1. System/software requirements

a) Authentification

1.	Is it ensured that no default passwords are applied?
2.	In the event of an unsuccessful login, does the product only display information that does not allow the user to identify the exact cause of the blocking, such as messages "wrong user name" or "wrong password"?
3.	Has the manufacturer established a concept for authorisations and, if applicable, roles for users and neighbouring systems?
4.	If available: Does the product allow each role to access only those functions for which it is authorised? (This also applies in particular to updating/upgrading the product).
5.	Does the product allow authorised users to block other users and neighbouring systems? Has the manufacturer defined risk-based measures that result in no safety risks?
6.	In a client-server architecture, are all IT security measures determined and checked on the server side? In a client-server architecture, are all client inputs checked on the server side?

b) Communication and storage

1.	How does the manufacturer ensure the integrity and confidentiality of data in the event of their transmission?
2.	How is the change of use or unintentional deletion of data prevented?
3.	If data is to be permanently deleted, how is it ensured that this happens?
4.	Does the product reject all unknown incoming connections (e.g. USB, TCP, Bluetooth) by default, based on application and risk?
5.	Does the product check all user inputs and all incoming data against manufacturer-defined verification criteria before further processing?
6.	Does the product store passwords in such a way that they cannot be reconstructed?
7.	Has the manufacturer defined and implemented protection for personal identifying characteristics?
8.	Has the manufacturer implemented measures to maintain the integrity of software and data?
9.	Does the product allow data interfaces to be deactivated / disabled?
10.	Is there a list of all recipients to whom data is transferred, with precise details of the type of data and any anonymization/pseudonymization to be carried out?
11.	Has it been identified which data (e.g. Google advertising ID) could lead to de-pseudonymization? How is this prevented?
12.	How is it ensured that the user is informed about the storage contents and locations of his or her data and gives his or her (documented) consent before the first transmission?
13.	Does the user have the possibility to object to certain transfers?

14.	Is the user informed about data transfers of any kind to storage locations that are not subject to EU data protection regulations and does he/she expressly consent to storage at these locations as well?
15.	What happens in the event of revocation/non-consent?
16.	In the context of risk management, are the consequences of compromise of each data location defined and what measures are taken to prevent this?

c) Patches

1.	Is there a system that allows patches to be applied and faulty patches to be removed?
2.	Is there an integrity check of the patches?

d) Logging

1.	Has the manufacturer defined where the log files are located, how they are protected, updated and in what form they can be (automatically) evaluated?
2.	Is there a risk-based logging concept that records significant changes to the product and events and protects against changes?

2. System/software architecture

1.	Does the software exclusively use proven libraries / components for all cryptographic functions (e.g. encryption, signing) or is a proprietary implementation comprehensively evaluated?
2.	Is the software based on the versions of the SOUP/OTS components that do not contain any security-relevant vulnerabilities? Are exceptions justified?

3. Accompanying materials

1.	Do the instructions for use specify the intended IT environment for operation?
2.	Do the instructions for use specify which activities the operators must perform, how and how often?
3.	Do the installation and service instructions specify which other roles (operators, service technicians) must perform which activities and how often?
4.	Do the accompanying materials describe how to deal with lost or stolen authentication elements (e.g. cards, certificates, cryptographic keys) and forgotten passwords?
5.	Do the accompanying materials describe how users can recognise that the product has an IT security problem and how they should act in this case?
6.	Do the accompanying materials describe which anti-malware software is approved for the product and from where (e.g. link) it can be obtained and who is responsible for updating it?
7.	Do the accompanying materials contain the manufacturer's contact details, which can be used to reach the manufacturer, e.g. in the event of problems with IT security?
8.	Do the accompanying materials also describe the product technically?

D) Supplementary aspects to be additionally addressed by the manufacturer within the context of risk management

1. System and software architecture

(Complement to ISO 14971, Annex C)

1.	Has the manufacturer identified the user (at operating system level) for each process and justified if it is not running with minimal rights ("worst case" as root)?
2.	Has the manufacturer systematically derived risks from a lack of IT security through threat modelling?
3.	Has the manufacturer analysed the risks arising from the (auto)update of anti-malware?
4.	Are any FPGAs included part of the risk analysis?
5.	Is the FPGA code obtained as IP core managed like libraries?
6.	Are update options provided for FPGAs that have been classified as security-relevant in the risk analysis?

2. Product release

1.	Has the manufacturer addressed the most common vulnerabilities and resulting hazards in the risk analysis and can demonstrate why these risks are controlled?
2.	Has the manufacturer considered the risks of all relevant attack vectors in the risk analysis and shows how these are controlled?
3.	Has the manufacturer checked all risk control measures for effectiveness and documented them?

E) Supplementary References

- 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 2019-11 - 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