WG(s):	DAISAM	E-meeting, 27-29 January 2021

DOCUMENT

Source:	Editors	
Title:	Updated DEL2.2: Good practices for health applications of machine learning: Considerations for manufacturers and regulators	
Purpose:	Discussion	
Contact:	Luis Oala HHI Fraunhofer Germany	Email: luis.oala@hhi.fraunhofer.de
Contact:	Christian Johner Johner Institute for Healthcare IT Germany	Email: christian.johner@johner-institut.de
Contact:	Pradeep Balachandran Technical Consultant (Digital Health) India	Email: pbn.tvm@gmail.com

Abstract: This document contains the latest draft of the FG-AI4H deliverable DEL02.2 "Good practices for health applications of machine learning: Considerations for manufacturers and regulators". This deliverable defines a set of guidelines intended to serve the AI solution developers/manufacturers on how to do conduct a comprehensive requirements analysis and to streamline the conformity assessment procedures to ensure regulatory compliance for the AI based Medical Devices (AI/ML-MD).

International Telecommunication Union

ITU-T   FG-AI4H Deliverable

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(draft 27-01-2021)

DEL2.2

Good practices for health applications of machine learning: Considerations for manufacturers and regulators

Summary

This technical paper recommends a set of good machine learning practice guidelines to the manufacturers and regulators of data driven Artificial Intelligence based healthcare solutions on conducting comprehensive requirements analysis and streamlining conformity assessment procedures for continual product improvement in an iterative and adaptive manner. This set of good machine learning practice guidelines gives prime priority to the factor of patient safety and focuses on a streamlined process for risk minimization and quality assurance for AI/ML based health solutions and tries to establish a system of transparency and accountability of all the processes involved in AI/ML based health solutions. The proposed set of good machine learning practices adopts, extends and leverages the best practices and recommendations provided by internationally recognized medical device regulatory agencies such as the IMDRF and the FDA. These guidelines are devoid any legally binding or statutory requirements applicable to any specific regulatory framework or specific geographic jurisdiction.

Keywords

Regulatory Checklist, Software-as-a-Medical Device, AI/ML based Medical Devices

Change Log

This document contains latest version of the Deliverable DEL2.2 on "*Good practices for health applications of machine learning: Considerations for manufacturers and regulators*"[approved at the ITU-T Focus Group on AI for Health (FG-AI4H) meeting held in(draft 27-01-2021)].

Editors:	LuisOala HHI Fraunhofer, Germany	Email: luis.oala@hhi.fraunhofer.de
	Christian Johner Johner Institute for Healthcare IT, Germany	Email: christian.johner@johner-institut.de
	Pradeep Balachandran Technical Consultant (Digital Health), India	Email: pbn.tvm@gmail.com
Contributors:	(in alphabetical order)	
	Aaron .Y. Lee University of Washington	Email:leeay@uw.edu
	Alixandro Werneck Leite Machine Learning Laboratory of Finance and Organizations, University of Brasilia, Brazil	Email: alixandrowerneck@outlook.com
	Andrew Murchison Company Oxford University Hospitals NHS Foundation Trust, United Kingdom	Email: agmurchison@gmail.com
	AnleLin,Health Sciences Authority, Singapore	Email: LIN_Anle@hsa.gov.sg
	Christoph Molnar Expert for Interpretable Machine Learning Technische Universität München	Email: Christoph.molnar@gmail.com
	Juliet Rumball-Smith New Zealand Ministry of Health	Email: juliet@rumballsmith.co.nz

Pat Baird
Philips, U S A

Email: pat.baird@philips.com

Peter. G. Goldschmidt
World Development Group Inc., USA

Email: pgg@has.com

Pierre QuartaroloDanish Medicines Agency

Email: jepq@dkma.dk

Shan Xu
China Academy of Information and
Communications Technology (CAICT)
China

Email: xushan@caict.ac.cn

Sven Piechottka
Merantix Healthcare
Germany

Email: sven.piechottka@merantix.com

Zack Hornberger
Medical Imaging & Technology Alliance

Email: zhornberger@medicalimaging.org

CONTENTS

Page

Page

List of Tables

Page

List of Figures

Page

ITU-T FG-AI4H Deliverable DEL2.2

Good practices for health applications of machine learning: Considerations for manufacturers and regulators

Background

Artificial Intelligence-based technologies find extensive use in medical applications and the proliferation of AI-based technologies holds great potential to improve the accessibility, quality, and value of healthcare outcomes. Regulation plays an important role in ensuring the safety of patients and users and in the commercialization and market acceptance of these AI-based medical devices. Therefore, streamlined and systematic regulatory compliance processes can help to expedite regulatory approval and to reduce the time-to-market for these products. AI-based medical devices are, by definition, software devices; and as per the International Medical Device Regulators Forum (IMDRF), a 'Software as a Medical Device (SaMD)' is defined as a software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device, where 'medical purposes' include diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of diseaseand other conditions. This document scope covers only data driven AI systems and does not take into account the aspects of non-data driven rule based /expert AI systems.

Machine Learning (ML) technologies, a subset of AI technologies, have the unique ability to learn from real-world feedback data and adapt their performance over time. The complexity introduced by these technologies is relevant to the clinical safety and performance of the medical device, and may introduce new risks or lead to modification of existing risks, which act as barriers to acceptance. Black box AI/ML–algorithms that resist comprehensive explanation–also create barriers to acceptance. These characteristics raise important technological, methodological, ethical, privacy, security, and regulatory issues, and there is an absolute need for reasonable assurance mechanisms to maintain and/or improve the performance, safety and effectiveness of AI/ML-based medical devices. Apart from these device-oriented issues, there are other challenges that include a lack of universally accepted policies and guidelines for regulation of AI/ML based medicals devices, which create barriers such as interoperability for these types of devices to scale up at the global level. Many medical devices companies do not have adequate awareness of machine learning best practices and standards and thus fail to assess the potential implications of safety, ethical and legal risks.

There is a need for proper guidance mechanisms to educate and train medical device manufactures to work to good practice guidelines applicable to AI/ML based devices. There is also need for regulatory policies and guidelines to be tailored for AI/ML based medicals devices. The main aim of these good machine learning practice guidelines is to safeguard patient safety as first priority through a streamlined process for manufacturers that will help ensure that products benefit patients by promoting health and minimizing risk. The proposed set of guidelines adopts, extend and leverage best practices and recommendations provided by the international medical device regulatory agencies such as the IMDRF and the FDA.

Target of this guideline

Aims

– To help manufacturers familiarize with international laws and regulations that applies to AI/ML-based medical devices and to bring them to market quickly and effectively.

– To help internal and external auditors test the legal conformity of AI/ML-based medical devices and the associated life-cycle process.

Objectives

The objective of this guideline is to provide target users with instructions and to provide them with a concrete checklist:

– To understand the expectations of the regulatory bodies

– To promote step-by-step implementation of safety and effectiveness of AI/ML based Software as Medical Device

– To fill the current gap in international AI/ML-based medical device standards to the greatest extent possible

Target audience

The following user classes/roles are deemed responsible for using the guidelines:

– quality assurance auditors / managers

– developers

– testers

– regulatory specialists

– data scientists

– clinical specialists

– physicians

– product managers

– medical device consultants

– risk assessment specialists

– service and support providers

1 Scope

This document defines a set of guidelines intended to guide the developers and manufacturers of healthcare AI solutions with requirements pertaining to good practices and processes for AI / ML based Medical Devices (AI/ML-MD) development.

This scope of the guidelines covers only data driven AI systems and does not take into account the aspects of non-data driven rule based /expert AI systems.

This set of guidelines promotes a common understanding between the manufacturers, the notified bodies and other pertinent authorities on the best practices to conduct a comprehensive requirements analysis and to streamline the conformity assessment procedures for continual product improvement in an iterative and adaptive manner in conformance to the appropriate standards and regulations

This set of guidelines is not intended to be a primer on artificial intelligence health applications or machine learning but is intended to serve as a resource guide for regulators when shaping regulations pertaining to AI/ML-MDs

The regulatory requirements scope of AI/ML-MD pertains only to technical aspects and functional safety & efficacy of its entire product life cycle; and not to commercial or business aspects, such as strategic positioning, market assessment, profitability, etc.

This set of guidelines is not intended 1) to be comprehensive and/or 2) to replace any regulation, directive, standard, or similar legally binding regulatory framework or guidance document of any geographic jurisdiction

The scope of AI/ML-MD:
– INCLUDES (a) regulated and non-regulated medical devices, (b) medical devices with or without enforcement of regulations

– INCLUDES (a) Software-as-a-Medical Device (SaMD), (b) Software-in-a-Medical Device (SiMD) and (c) healthcare applications intended to improve medical outcomes or efficiency of healthcare system

– INCLUDES both (a) Static AI model-based systems(b) Continuous/Incremental learning AI/ML model-based systems

– DOES NOT INCLUDE software applications for (a) healthcare facility administrative support, (b) for maintaining or encouraging healthy lifestyle, behaviour and wellness

Regulatory Guidelines: classification criteria for scope definition

For defining the applicability scope of the proposed guidelines, classification criteria based on a) scope of regulation, b) scope of product and c) scope of application are used. The classification criteria & scope of the proposed guidelines is illustrated in Figure 1.
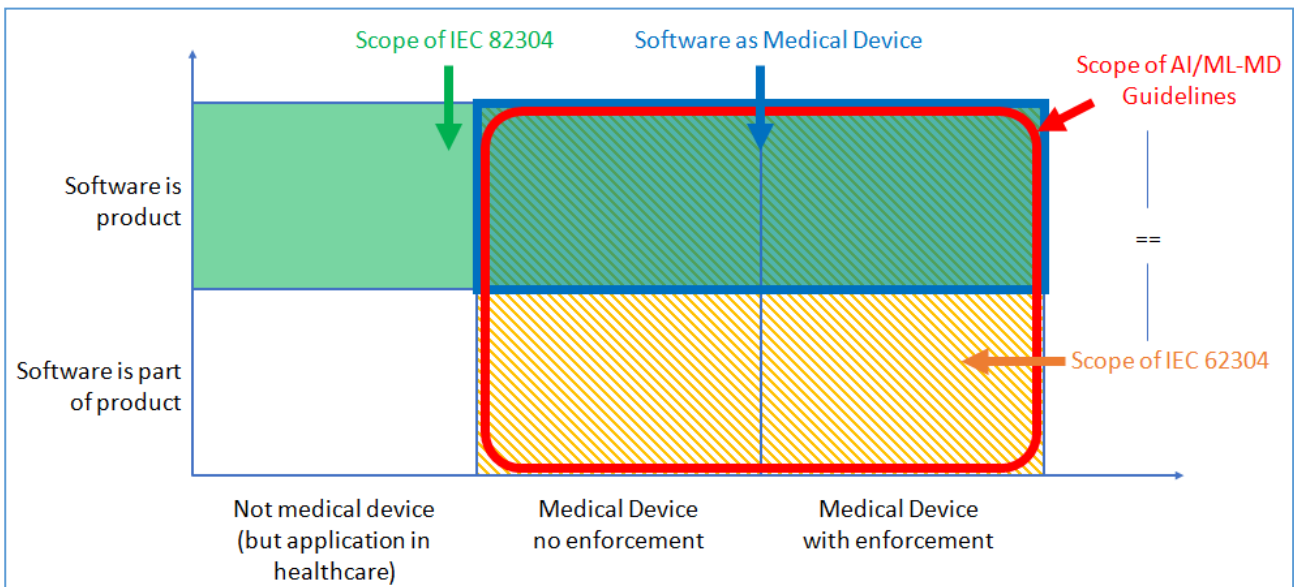
Figure 1: AI/ML-MD Classification Criteria & Scope

Regulatory scope

Medical device:
– with enforcement of regulations

– without enforcement of regulations.

Product scope
– software is the product ->standalone software –Software-as-medical device (SaMD)

– software is embedded in the product- Software-in-medical device (SiMD)

Application scope

In healthcare:
–   to improve medical outcome (e.g. to support diagnosis, treatment, prevention, monitoring and prediction of diseases and injuries)

–   to improve workflow efficiency (e.g. AI recommender systems for 'clinical process' efficiency improvement', NLP pipeline based unstructured clinical data analysis to alert treatment preparations and monitoring of adverse effects, etc.)

2   References

The following list of reference documents were reviewed as part of broad literature survey towards the design of the proposed regulatory requirements guidelines, considering aspects of regulations, standards, guidelines, best-practices, directives and laws that are relevant in the context of AI-MD. A detailed list of regulatory references considered towards the formulation of the proposed guidelines is included in Annex C: Relationship to other guidelines and standards

[EU-MDR (2017/745)]	REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (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.
[FDA 21 CFR]	FDA 21 CFR part 820, Quality System Regulations
[FDA]	Guidance "General Principles of Software Validation"
[FDA]	FDA's "Proposed Regulatory Framework for Modifications to Artificial Intelligence / Machine Learning (AI/ML) Based Software as Medical Device
[GDPR]	European General Data Protection Regulation
[GHTF/SG5/N1R8:2007]	Clinical Evaluation, SG5/N2RR-2007, Global Harmonization Task Force
[GHTF/SG1/N71:2012]	Definition of the Terms 'Medical Device' and 'In Vitro Diagnostic (IVD) Medical Device', GHTF/SG1/N071:2012,Global Harmonization Task Force
[IEC 62304]	IEC 62304:2006 + A1:2015, "Medical device software – Software life cycle processes"
[IEC 62366]	IEC 62366-1:2015, "Medical devices – Part 1: Application of usability engineering to medical devices"
[IEC 82304]	IEC 82304-, "Health software – Part 1: General requirements for product safety"
[IMDRF/GRRP WG/N47]	IMDRF/GRRP WG/N47 Final (2018), "Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices"
[ISO 13485]	ISO 13485:2016, "Medical devices – Quality management systems – Requirements for regulatory purposes"
[ISO 14971]	ISO 14971:2019, "Medical devices – Application of risk management to medical devices"

[ISO 9241-11]	ISO 9241-11, " Ergonomics of human-system interaction –Part 11: Usability: Definitions and concepts"
[ISO 9241-210]	ISO 9241-210, " Ergonomics of human-system interaction –Part 210: Human-centred design for interactive systems"
[ISO 14155]	ISO 14155, " Clinical investigation of medical devices for human subjects – Good clinical practice"
[ISO/IEC 27000]	ISO/IEC 27000, " Information technology – Security techniques – Information security management systems – Overview and vocabulary"
[ISO/IEC 27002]	ISO/IEC 27002, "Information technology – Security techniques – Code of practice for information security controls"
[ISO/IEC 27002:2013]	ISO/IEC 27002:2013, "Information technology – Security techniques – Code of practice for information security controls, TECHNICAL CORRIGENDUM 1"
[ISO/IEC 27002:2013]	ISO/IEC 27002:2013, "Information technology – Security techniques – Code of practice for information security controls, TECHNICAL CORRIGENDUM 2"

3 Terms and definitions

3.1 Terms defined elsewhere

This document uses the following terms defined elsewhere:

3.1.1 Artificial Intelligence (AI) [ISO/IEC 22989, 3.2.1.2]: capability of an engineered system to acquire, process and apply knowledge and skills (Note 1 to entry: knowledge are facts, information, and skills acquired through experience or education).

3.1.2 AI system [ISO/IEC 22989, 3.2.1.4]: technical system that uses artificial intelligence to solve problems.

3.1.3 Clinical Evaluation [GHTF/SG5/N1R8:2007]: The assessment and analysis of clinical data pertaining to a medical device to verify the clinical safety and performance of the device when used as intended by the manufacturer.

3.1.4 In Vitro Diagnostic (IVD) Medical Device [GHTF/SG1/N71:2012]: A medical device, whether used alone or in combination, intended by the manufacturer for the in-vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes.

3.1.5 Lifecycle [ISO/IEC Guide 51:2014]: All phases in the life of a medical device, from the initial conception to final decommissioning and disposal.

3.1.6 Machine Learning [ISO/IEC 23053, 3.16]: process using computational techniques to enable systems to learn from data or experience.

3.1.7 Medical Device [GHTF/SG1/N71:2012]: Any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of: a) diagnosis, prevention, monitoring, treatment or alleviation of disease, b) diagnosis, monitoring, treatment, alleviation of or compensation for an injury, c) investigation, replacement, modification, or support of the anatomy or of a physiological process, d) supporting or sustaining life, e) control of conception, f) disinfection of medical devices, g) providing information by means of in vitro examination of specimens derived from the human

body; and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means.

3.1.8   Software as a Medical Device [IMDRF/GRRP WG/N47]: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.

3.1.9   Software Validation [IEEE-STD-610]: The process of evaluating software during or at the end of the development process to determine whether it satisfies specified requirements.

3.1.10   Software Verification [IEEE-STD-610]: The process of evaluating software to determine whether the products

3.2   Terms defined in this document

This document does not define any terms.

4   Abbreviations and acronyms

This document uses the following abbreviations and acronyms.

AI	Artificial intelligence
AI4H	Artificial intelligence for health
AI/ML-MD	Artificial Intelligence / Machine Learning based Medical Devices
CSV	Computerized Systems Validation
DAISAM	Data and AI Solution Assessment Methods
EP	Essential Principle
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IMDRF	International Medical Device Regulators Forum
ITU	International Telecommunication Union
IVD	In vitro diagnostics
MDD	Medical device directives
MDR	Medical device regulation
ML	Machine Learning
ML4H	Machine Learning for Health
SaMD	Software-as-a-medical device
SiMD	Software-in-a-medical device
WG	Working group
WHO	World Health Organization

5   Conventions

None.

6   General requirements

6.1   Process requirements

Table 1: Process requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s)applicable
PROC-1	The manufacturers should establish a quality management (QM) System that covers all life cycle phases.	– There is at least one SOP[1] covering the design& development process including verification and validation. – There is/are SOP(s) covering the post-market surveillance and vigilance. – There is a SOP covering risk management. – There is a SOP covering Computerized Systems Validation (CSV). – There is a SOP covering the data management (process). – There is/are SOP(s) covering software delivery, service, installation, decommissioning. – There is a SOP covering customer communication		EU-MDR (2017/745) Article 10.9 ISO 13485 e.g. clause7.1 ISO 13485 clause4.1.6 21 CFR part 820

---

[1]Standard Operating Procedure. All SOPs have to be approved and be under version control.

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s)applicable
		including handling of customer complaints.		
PROC -2	The manufacturer should compile all product specific plans as required by respective regulations.	– There is a product specific development plan (including verification and validation). – There is a product specific post-market surveillance plan. – There is a product specific clinical evaluation plan. – There is a product specific documented risk management plan.		MDR (2017/745) Annex I (3) MDR (2017/745) Annex III (1.3) IEC 62304 clause5.1 ISO 14971:2019 (4.2) 21 CFR part 820.30(b) FDA SW validation guidance 5.2.1

6.2 Competency requirements

Table 2: Competency requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
COMP-1	The manufacturer should identify the roles inside the scope of its QM system that is directly or indirectly concerned with AI.	– There is a list that specifies roles and responsibilities inside the manufacturer's organization involved in its product life cycle activities. – These roles include software developers, software testers, data scientists, experts of	Examples for domain experts are physicians, clinicians, nurses, lab technicians, pharmacists etc. Additional roles may include the following:	ISO 13485 clause 5.5.1 ISO 13485 clause 6.2 EU MDR (2017/745) Article 10.9 21 CFR part 820.30(b) FDA SW validation guidance 5.2.1

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		clinical evaluations, risk managers, usability engineers and domain experts.	– regulatory affairs and quality managers – product managers – medical device consultants – service technicians e.g. update, upgrade, configuration, installation, capturing audit logs, etc. – support staff.	
COMP -2	The manufacturer should ensure the necessary competencies for each role inside the scope of its QM system that is directly or indirectly concerned with AI.	– There are documented competency requirements for each role. – There is a documented procedure on user role training and allied training materials. – There are records that provide evidence that the competency requirements have been met.	Examples of competencies are related to: – education – knowledge – skills: Capability to perform a particular task. Examples for training records are: – (self) tests – artefacts that result from practicing a particular skill e.g. documents.	ISO 13485 clause 6.2. ISO 14971:2019 clause 4.3 ISO 13485:2016 clause 7.3.2 IEC 82304 clause 6.1 FDA: Culture of quality and organizational excellence: "Continuous development of employees through robust knowledge management, employee development options, coaching, training, and succession planning. " (s. pre-cert program)

7 Pre-market requirements

7.1 Intended use and stakeholder requirements

7.1.1 Intended medical purpose

Table 3: Intended use requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
USE-1	The manufacturer should determine the medical purpose of the medical device.	There is documented specification of: – Indication including disease or injury or physiological state, – Goal: e.g. diagnosis, treatment, monitoring, prevention, elevation and / or prognosis.	The disease or injury is specified using ICD-10 codes (at least 3 digits). Increasing adherence is an example for improving treatment. The description answers questions like – Is it a self-contained device with application or an operational supporting system? – Is it health related or operations support?	MDR (2017/745) Annex II (1.1) ISO 13485 clause 4.2.3 ISO 14971:2019 clause 5.2 21 CFR 814.20 (b)(3)(i) 21 CFR part 820.30(c)
USE--2	The manufacturer should specify other positive impacts on health care.		– Faster patient care e.g. treatment, diagnosis. – Reductions in workload. – Reductions in costs of healthcare.	MEDDEV 2.7/1 rev. 4 MDR (2017/745) Annex I (23.4) FDA guidance on "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval"

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
USE--3	The manufacturer should specify the target patients.	There is a documented specification of: – demographics (e.g. age, sex) – Indications – contraindications – co-morbidities.	Comment: The intended use has to be specified in relevant detail for all pertinent aspects. Certain derivative requirement would pertain only to the specified uses. E.g., if the product is intended to support diagnosis in white women, there is no need to know the product's performance in black men. There might be a requirement to warn users to restrict use of the product to white women.	MDR (2017/745) Annex I (23.4) MDR (2017/745) Annex II (1.1) IEC 62366-1clause 5.1 21 CFR 814.20 (b)(3)(i) FDA guidance on "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval"
USE--4	The manufacturer should specify the intended part of body or type of tissue the medical device shall interact with.			IEC 62366-1clause 5.1
USE--5	The manufacturer should specify the operating principle.	– There is a description of the task the ML-model may perform. – There is a specification of the type machine learning. – There is a description whether an intervention of the user before treatment or diagnosis is necessary, possible, not possible.	Typical tasks include: – segmentation – detection – decision support – recommendation – process automation – search (e.g. similarities). Typical dimensions include: – Type of learning (supervised,	IEC 62366-1clause 5.1 MDR (2017/745) Annex II (1.1) 21 CFR part 814.20 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA Proposed Regulatory Framework for Modifications to Artificial

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− There is a clarification whether the AI trigger an autonomous action/decision or just provides information for human analysis − There is a description of the level of independence	unsupervised, semi-supervised, reinforcement), − Time and type of learning (before placing on the market→ locked algorithm, during use, globally, per product instance, per hospital), − Technical task (classification, regression, clustering, control). XAVIER differentiates these user interactions: − intervention before treatment or diagnosis is not possible − intervention before treatment or diagnosis is possible by overriding − intervention before treatment or diagnosis is necessary by approval − there is no direct diagnosis or treatment possible with the system.	Intelligence/Machine Learning (AI/ML)-Based SaMD
USE--6	The manufacturer should provide explicit task	− Background information, including a review of the evidence, the purpose of the		

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	description by distinguishing it from the particular algorithm used	task, all relevant definitions, and discussion of limitations and special cases; − A thorough description of the diagnostic task, including criteria for making the clinical assessment, descriptions and definitions of the measurement, or a description of all classification categories. − Detailed image labelling instructions for the task, including specific labelling strategies and relevant pitfalls. − Illustrated prototypical examples and relevant counter- examples, such as an atlas.		

7.1.2 Intended users and context of use

Table 4: Intended users and intended context of use specification

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
ENV-1	The manufacturer should characterize the intended users.	– There is a list of intended primary and secondary users. – The characteristics and prerequisites that each user group has to fulfil are specified.	User characteristics my include: – education – experience in medical domain – technical skill knowledge – training to be accomplished – physical prerequisites and limitations (height, sight, disabilities) – intellectual and mental prerequisites and limitations – language skills – experience with product type or technology – cultural and social background.	MDR (2017/745) Annex I (5) MDR (2017/745) Annex II (1.1) IEC 62366-1clause 5.1 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA Guidance "Applying Human Factors and Usability Engineering to Medical Devices" (chapter 5.1)
ENV -2	The manufacturer should characterize the intended use environment.	There is a documented specification of the: – physical use environment – social use environment – work environment.	The physical environment might include: – brightness – loudness e.g. alarms – temperature	MDR (2017/745) Annex I (5) IEC 62366-1clause 5.1 XAVIER University "Building

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			− contamination − visibility − humidity, moisture. The social environment may include: − stress, mental workload − shift operation − number of people and frequently changing colleagues. The work environment may include: − wearing of gloves or other personal protection equipment − usage of tools − physical stress.	Explainability and Trust for AI in Healthcare" FDA Guidance "Applying Human Factors and Usability Engineering to Medical Devices" (chapter 5.2) ISO 13407-Human-centred design process for interactive systems
ENV -3	The manufacturer should specify the product lifetime.		The product lifetime may depend on: − technologies applied in the product − technical environment such as operating systems, browsers, networks − development of the state of the art e.g. progress in medical research	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			− competitive products.	

7.1.3 Stakeholder requirements

Table 5: Stakeholder requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
STKH-1	The manufacturer should operationalize the goals listed in the intended use with quantitative values for product	− There are documented user requirements. − There are documented quantitative performance requirements.	Examples of user requirements: − 95% of radiologists working with system detect the cancer. Examples of performance requirements: − the system shall have a sensitivity of 97% − the system must be able to detect coronary artery plaques of at least 0.2 mm diameter.	MDR (2017/745) Annex I (23.4) MDR (2017/745) Annex III (1.1) FDA SW validation guidance 5.2.2 FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (s.

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			Comment: For different sub-groups there might be different specifications of performance requirements.	"Software Requirements Specification")
STKH -2	The manufacturer should specify the runtime environment of the product regarding hardware and software.	− It is specified whether the software runs inside a medical device, as mobile app, as wearable device, as desktop application, in the cloud or another environment. − The minimum hardware requirements are specified. − The minimum software requirements are specified.	Hardware requirements may include: − CPU − RAM − screen size, resolution and orientation − physical storage − network connectivity e.g. bandwidth, latency, reliability − required peripherals such as printers, scanners, input devices − Sensors − Energy source − Periphery (keyboard, mouse etc.) − AI acceleration hardware/ inference acceleration hardware Software requirements may include: − operating system (incl. version) − browser (type, version)	ISO 13485 clauses 7.3.3 EU MDR (2017/745) Annex 1, 17.3 and17.4 IEC 62304 clause 5.2 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA SW validation guidance 5.2.2 FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (s. "Software Requirements Specification")

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			– virtualization (e.g. Java Runtime Environment, NET, Docker, virtual machines).	
STKH -3	The manufacturer should identify and specify the data interfaces.	– There is a list of data interfaces (can be specified in a context diagram as well). – The protocols are specified. – The formats are specified. – The semantic standards are specified.	Protocols might include: – OSI-Protocols such as TCP/IP, HTTPS – Bus-Systems such as CAN – Wireless communication protocols (Bluetooth, 4/5G cellular, Wi-Fi, etc) – physical hardware connections(e.g. USB) Format might include: – file formats (XML, JSON, PDF, docx, CSV, DICOM) – image formats (size, resolution, colour coding). Semantic standards might include: – taxonomies e.g. ICD-10, ATC – nomenclatures e.g. LOINC – information exchange e.g. FHIR, DICOM, HL7, etc	IEC 62304 clause 5.2 FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (s. "Software Requirements Specification")
STKH -4	The manufacturer should specify the requirements for input data for each inbound data interface.	There is a specification of input data.	Input data specifications may include: – ranges – data types – sensor requirements	IEC 62304 clause 5.2 ISO 14971:2019 clause 5.3 FDA Guidance for the Content of Premarket Submissions for

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			− type of data capturing device − precision of data − size/ quantity of data − type and technical parameters of recording procedure (e.g. strength of magnetic field, number of electrodes. − frequency of data	Software Contained in Medical Devices (s. "Software Requirements Specification")
STKH -5	The manufacturer should determine the regulatory requirements.	− There is a list of countries / markets that the product may be place in. − There is a list of laws, standards, regulations, directives, guidance.	The list might include documents such as: − FDA guidance documents − standards (e.g. IEC 62304, ISO 13485) − laws and regulations e.g. MDR (2017/745), IVDR.	MDR Annex IX (2.2) ISO 13485 (clauses 5.2 and 7.2.1)

7.1.4 Risk management and clinical evaluation

Table 6: Inputs to risk management and clinical evaluation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
RSK_MGNT_1	The manufacturer should evaluate alternatives to the given product (e.g. other products, procedures, technologies) and	− There is a clinical evaluation.	Alternative technologies might include: − other ML models	MEDDEV 2.7/1 MDR (2017/745) Annex I 1.

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	establish the necessity for using machine learning models.	− The clinical evaluation lists alternative products, technologies and/ or procedures. − There is a search protocol revealing how the manufacturer was searching for alternatives. − The clinical evaluation assessing alternatives with respect to clinical benefits, safety / risks, performance. − The alternatives include non-ML based technologies. − There is a statement confirming that the product reflects the state-of-the-art.	− non-ML methods e.g. classical algorithms.	ISO 14971:2019 clauses 4.2 and 10.9 FDA guidance on "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval" (e.g. Part C)
RSK_MGNT_2	The manufacturer should compile a list of risks specifically associated with the use of the method of machine learning.	− The risk management file contains an analysis of hazards and related harms with related probabilities and severities resulting from ML models not meeting the requirements. − There is a FMEA that analyses the effects of ML models that do not meet the performance requirements.	Performance requirements might include: − accuracy − specificity − sensitivity − response times − robustness − other Comment: differential performance by patient demographics	ISO 14971:2019 clauses5.4 and 5.5 EU MDR (2017/745) Annex 1 (3) DIN SPECT 2 ISO/TR 31004:2013 - Risk management - Guidance for the implementation of ISO 31000

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
RSK_MGNT_3	The manufacturer should analyse the reasonably foreseeable risks.	The risk management file analyses risks associated with: – non-specified users – non-specified use environment – application of product for patients other than those specified – reasonably foreseeable misuse – hardware failure	Non-specified users: – other profession e.g. nurse instead of physician – missing training. Other patients: – different age, sex, race – other co-morbidities – different severity of disease or injury Comment on 'reasonably foreseeable risks': This is significant. Particularly with respect to perpetuating/maintaining historical biases in treatment/service according to race/ethnicity, or historical issues around systematic misdiagnosis or under investigation in certain groups.	MDR Annex I 14.2 d) ISO 14971:2019 clause 5.2 DIN SPECT 2 21 CFR part 820.30(g) FDA guidance on Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices IEC 31010:2019 - Risk management - Risk assessment techniques

7.2   Product and software requirements

7.2.1   Functionality and performance

Table 7: Functionality and performance requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable

FNCT-1	The manufacturer should derive traceable quantitative quality criteria and requirements for the software and/or the algorithm from the intended use and from the stakeholder requirements.	– There is a specification of quantitative minimum 'quality criteria'.
		 – There is 'traceability matrix' that links the intended use with quantitative quality product requirements.
			'Quantitative quality criteria' may include the following:
			 – for classification problems:
			    o accuracy (mean or balanced accuracy)
			    o positive and negative predictive value in the intended use population
			    o specificity and sensitivity
			    o F1 Score Area under the ROC curve (AUC)
			    o Area under the Precision-Recall Curve
			 – for regression problems:
			    o mean absolute error
			    o mean square error
			    o Bland-Altman plot-difference measure (for bias estimation)
			
			 Note: Further metrics can determine how stable ("non-
				IEC 62304 clause 5.2
				 ISO 13485 7.3.3
				 XAVIER University "Building Explainability and Trust for AI in Healthcare"
				 FDA guidance on "Software Validation", chapter 5.2.2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			distractible") and deterministic the model has to be. Example 1: The stakeholder requirement states that 95% of radiologists must be able to detect a cancer with the product. The requirement of the algorithm states that it must display a sensitivity of 97%. Example 2: The stakeholder requirements state that arterial calcification must be able to be detected at a sensitivity of 92%. The requirements of the algorithm state that it must be able to exactly predict the strength of the plaques in the blood to 0.2 mm. Comment: They should be able to show that the model is equally accurate for different groups of patients Note: "Stability" can be understood from the point of view of *conditioning analysis (conditioning number via Eigen values) *functional analysis (e.g. through Lipschitz continuity)	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			*epsilon-based robustness as in adversarial research *robust statistics as proposed by Huber	
FNCT -2	The manufacturer should derive non-functional requirements from the intended use and stakeholder requirements.	There is a specification of non-functional requirements such as: – repeatability / reproducibility – response times – data volumes to be handled – availability – security e.g. access restrictions	Self-tests can be a mean to verify the repeatability of a system. The specification of response times might depend on number of users, number of transactions, frequency and amount of input data etc. Availability can be expressed as percentage of time, percentage of usages or as meantime between failure.	ISO 13485 clauses 7.2.1 and 7.3.3 ISO 25010 MDR Annex I (17.1) XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA guidance on "Software Validation" chapter 5.2.2 Annex C- IT security Guidelines
FNCT -3	The manufacturer shall derive from risk analysis product/software requirements to minimize risk.	There is a risk table correlating risks and measures.	The risk table sometimes is referred to as "FMEA table" Examples for measures are – Kill switch, overruling thru human intervention – Redesign of user interface (s. user interface requirements) – Locked algorithm instead of continuous learning system – Restriction of intended use	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			– Validation of input data (see next requirement) – Backup, recovery – Redundant design, failover system e.g. without ML functionality	
FNCT -4	The manufacturer should specify how cyber-security risk management was incorporated in the device development lifecycle and what risk controls were implemented to ensure that all interfaces of the product and its communication channels are secured from potential cyber threats. Note that the scope includes protection of the software and protection of the datasets.	There is specification on – list of steps on how to identify and evaluate threats and vulnerabilities, control security risks, and monitor the efficacy of these controls – repeatable, reproducible, testing-oriented criteria to assess a device's cyber vulnerabilities, fight malware, and test the security measures		AAMI TIR 57: Technical Information Report 57 (TIR57), "Principles for Medical Device Security–Risk Management," UL 2900 Standard. New standard for software cyber-security for network-connectable products. 2017 Annex C- Cyber-security OECD Guidelines for the Security of Information Systems and Networks

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
FNCT -5	The manufacturer should determine how the system behaves if the inputs do not meet the specified requirements.	There is a specification that describes how the system reacts on: – adulterated data (integrity problem) – conflicting data – incomplete data sets – missing data, empty data, lack of data sets – wrong data format – excessive data quantities (amount, frequency) – data outside of specified value ranges – wrong temporal sequence of data, etc.		ISO 25010 IEC 62304 clause 5.2 ISO 14971:2019 clause 5.4 FDA guidance on "Software Validation" chapter 5.2.2 FDA digital health criteria
FNCT -6	For continuous learning systems the manufacturer should specify the frequency of algorithms updates.	It is specified what triggers updates.	Triggers include: – on availability of enough data – periodically – if a minimum change to the algorithm/output is exceeded continuously.	XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA proposed regulatory framework for modifications to AI/ML based SaMD e.g. Annex B
FNCT -7	For continuous learning systems the manufacturer should specify	There is a specification how data are cleaned e.g. by:		XAVIER: "Perspectives and Good Practices for

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	how quality control of new data is performed.	– correction – omission – user interaction.		AI and Continuously Learning Systems in Healthcare" FDA proposed regulatory framework for modifications to AI/ML based SaMD: ACP e.g. page 11
FNCT -8	For continuous learning systems the manufacturer should specify a range within changes to the algorithm and to system output are permitted.	There is a description of how: – algorithms are changed over time – the amount of change is quantified – these changes relate to changes to the output.	For example, a change to a neural network can target: – fit parameters such as weights of neurons or cut-off of activation function – hyper-parameters such as numbers of neurons per layer and number of layers. Note: CL systems exhibit "drift" as learn. They can eventually fall into very different local minima than the original model.	XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare" FDA proposed regulatory framework for modifications to AI/ML based SaMD: SPS e.g. page 10
FNCT -9	For continuous learning systems the manufacturers should specify how changes to the algorithm are controlled.	There is a specification of: – system self-checks on performance – functionality to enforce, prevent, delay or roll-back changes to algorithms – change reports, change/audit-logs	The decision whether to enforce, prevent, delay or roll-back changes by users or the manufacturer must be taken risk-based. The version control has to apply to the entire model including fit parameters, hyper-parameters,	XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare" ISO 24028 FDA proposed regulatory

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− control of versions of the algorithms − boundaries of autonomous learning	and model architecture with respective time stamps.	framework for modifications to AI/ML based SaMD ACP e.g. page 11

7.2.2 User interface

Table 8: User interface requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
UI-1	The manufacturer should specify what the user interface must display in case of error e.g. if the inputs do not meet the specified requirements.	There is specification of the user interface in case of: − incorrect data inputs (s. "The manufacturer should determine how the system behaves if the inputs do not meet the specified requirements") − internal errors.	See previous checklist item. UI output display modes may include the following: − warning − alert − caution − meantime between failure, etc.	MDR Annex I clause 5 IEC 62304 clause 5.2 FDA HFE guidance FDA guidance on software validation e.g. chapter 5.2.3
UI-2	For continuous learning systems the manufacturer should specify how the user is informed about significant changes to algorithms.	There is a specification of user interface parts that provide: − information that an algorithm change was performed or will be performed Note: For the user to have the option to reject, delay		XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare"

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– the user the option to reject, delay or roll-back an algorithm change.	or roll-back an algorithm change, all the previous versions of the ML model would need to be maintained	FDA proposed regulatory framework for modifications to AI/ML based SaMD: ACP e.g. page 11
UI-3	The manufacturer should determine whether there is a need for instructions for use and training materials.	Either there is an Instructions-for-Use (IFU) or the user risk analysis reveals no risks that can be further mitigated by an IFU.		MDR (2017/745) Annex I (23) FD&C, 21 CFR parts 801 and 820.120 ISO 13485:2016 clause 4.2.3

7.2.3 Additional software aspects

Table 9: Additional software requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
SFTW-1	The manufacturer should set forth requirements to detect internal errors.	The risk analysis considers risk that are caused by internal errors. The device specification specifies how manufacturers or service technicians can gain access to internal errors.	Examples of interfaces include: – data and user interfaces to audit logs – monitoring ports. Examples of internal errors are: – runtime errors such as null pointer exception	MDR (2017/745) Annex I (17, 18, 23.4) IEC 62304 clauses 5.2, 5.3 and 7.1 ISO 149781:2019 clause 5.4 FDA guidance on software validation e.g. chapter 5.2.2, 5.2.3 and 5.2.4

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			− resource overload such as out of memory errors − lack of access to resources such as databases − compromised integrity of data and program code.	
SFTW-2	The manufacturer should justify if the device takes decisions exclusively based on automatic data processing.	− There are records of processing activities. − There is a data protection impact assessment.		Art. 22 of the GDPR. Exceptions of Art. 22 section 2 may apply.

7.2.4   Risk management

Table 10: Risk management & clinical evaluation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
RSK_MGNT_4	The manufacturer should assess the risks arising if the inputs do not meet the specified requirements.	− There is an assessment which inputs and combinations of inputs of the input space have an (undesirable) impact on the system's output.	Invalid/ non-compliant input conditions may include the following: − incomplete data sets − lack of data sets − wrong data format − excessive data quantities	ISO 14971:2019 clause 5.4 IEC 62304 clause 7.1 DIN SPEC 2 IEC 82304 clause 4.1.c)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− The risk analysis assesses the risks for wrong inputs at each data interface. − The risk analysis considers all relevant types of wrong inputs. − There is an assessment of values or ranges for quality metrics that have to be met in order to avoid inacceptable risks. − The risk analysis considers a drift in data. − The risk analysis assesses risk by lack of robustness e.g. for adversarial attacks − There are adversarial examples defined that lead to inacceptable risk and that have to be evaluated in testing.	− data outside of specified value ranges − unreasonable combination of data (feature) − wrong meta-data − data drifts can be identified by mean values, distributions. Critical drifts can occur either in single features or combinations of feature − use of synonyms in texts − typing errors − malicious attacks e.g. by manipulating a few pixels in images.	
RSK_MGNT_5	The manufacturer should set the gold standard against which the quality criteria can be reviewed and justify their choice.	− The clinical evaluation lists alternatives. − The clinical evaluation compares these alternatives with respect to specified quality criteria.	The gold standard is not the same as alternatives. E.g. the gold standard to determine the blood pressure is an invasive measurement. But this is not the alternative.	XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA proposed regulatory framework for modifications to

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− There is a documented justification for the selected ground truth.		AI/ML based SaMD: "reference standard"
RSK_MGNT_6	The manufacturer should analyse the risks arising if the outputs do not meet the specified quality criteria.	There is risk assessment report / risk table that specifies risks in case outputs do not meet the specified 'quantitative quality criteria'.		ISO 14971:2019 clause 5.3 IEC 62304 clause 7.1 IEC 82304 clause 4.1.c) XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA guidance on software validation e.g. chapter 5.2.2
RSK_MGNT_7	The manufacturer should assess the consequences if the system provides socially unacceptable / discriminatory outputs.	There is of outputs that an assessment report on consequences / implications of socially unacceptable outputs. Assessment report includes: − cost estimation for wrong clinical decision making − AI autonomy level assignment and associated risk acceptance criteria based on criticality of the clinical use case and environment.		Ethics guidelines for trustworthy AI

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
RSK_MGNT_8	The manufacturer should assess the risk arising if the system does not meet the specified non-functional requirements.	The risk analysis assesses risk arising from: – lack of availability / robustness – slow response times – interoperability problems – software using more CPU, GPU, RAM, I/O, bandwidth than specified.		MDR Annex I 17.2 ISO 14971:2019 chapter 5.3 IEC 62304 clause 7.1 FDA guidance on software validation e.g. chapter 5.2.2
RSK_MGNT_9	The manufacturer should analyse risks if (run-time) environment does not meet the specifications.	The risk analysis assesses risk from: – insufficient or faulty hardware – software environment not meeting the specifications – network environment not meeting the specifications – interfaces not meeting the specifications.	Hardware related risks: – CPU, RAM, I/O, hard disk space not as specified – memory, CPU, GPU flaws – hard disk full – RAM, CPU, I/O overutilization by other applications. Software related risks: – other type or version of operating system, browser, virtualization layer (.NET, JRE, VM), libraries – software patches not installed – software bug.	MDR Annex I e.g. mobile platforms, network characteristics, e.g. 14.2.d) DIN SPEC 2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			Network related risks: − bandwidth, latency not as specified − endpoints, protocols not supported or blocked. Interface related requirements: − S. wrong input data − unspecified data volumes and frequencies.	
RSK_MGNT_10	The manufacturer should identify use related risks.	The risk analysis assesses risks caused by users: − not following the instructions for use − not understanding warnings and explanations − using the system in a technical of social environment that does not meet the specifications.	− User does not update the system. − User installs software on wrong. − User connects product to other systems not meeting requirements.	IEC 62366-1, chapter 5.3f. FDA HFE guidance FDA guidance on software validation e.g. chapter 5.2.3
RSK_MGNT_11	The manufacturer should analyse risks from malicious / adversarial attacks	- There is an analysis of potential attackers and motivation - There is a list of attack vectors - There is a vulnerability analysis	− Potential attacks are manipulating input data such as images or even of (public) training data ("poisoning attack") − The vulnerability increases if the attacker has access to the model	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			internals (e.g. architecture) or even to the model itself. Also, the chance of accessing the model via an API and thereby evaluating different attacks increases the vulnerability	
RSK_MGNT_12	With Continuous Learning Systems, the manufacturer should mitigate risks that are specific to continuously learning systems.	− The risk analysis assesses risks that a specific to continuous learning systems. − The risk management file specifies the respective risk mitigation.	Examples of risk mitigation: − option to reset the systems − self-tests.	MDR (2017/745) Annex I (17) FDA proposed regulatory framework for modifications to AI/ML based SaMD (entire document)
RSK_MGNT_13	With Continuous Learning Systems, the manufacturer should show quantitatively why the risk-benefit analysis is better than for non-continuously learning systems.	Analysis report showing a positive risk-benefit ratio compared to the state-of-the art. The clinical evaluation compares benefits for continuously learning and non-continuously learning systems.		ISO 14971:2019 clause 6 DIN SPECT 2 FDA guidance on determining benefit risk
RSK_MGNT_14	The manufacturer should mitigate risks.	There is a risk mitigation for risks caused by: − input data not meeting the requirements − inability of the system to meet the non-functional requirements	Means for risk mitigation might include: − System shutdown − Warnings to users, alarm systems − Validation of input data − Self-tests	ISO 14971:2019 clause 7 DIN SPEC 2 DAISAM FDA guidance on software validation e.g. chapter 6.1

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− ML algorithms not meeting the quality metrics − Adversarial attacks − software bugs. The measures are implemented: − The measures are specified as product or component requirements − There are tests verifying/validating the implementation and effectiveness of these measures.	− Robustness: Adversarial training (*arXiv:1706.06083*), *generative methods (See section "uncertainty" in DISAM paper)* − Adversarial attacks: Training with adversarial data sets or operating with different classifiers or learning invariant transformation of feature	FDA HFE guidance e.g. chapter 8.1.3 and 8.1.4 ISO 24028 10.4, 10.5, 10.7 ff.
RSK_MGNT_15	The manufacturer should repeat these risk management activities after training of the model as well as prior to product release.			

7.3 Data management requirements

7.3.1 Data collection

Table 11: Data collection requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
DAT_CL-1	The manufacturer should specify the number of required data sets.	− There is a specification of number of data sets. − There is a rationale for this number.	The division into training, test and validation data sets is scope of chapter 7.4.1.	ISO 13485 clause 7.3.7 FDA proposed regulatory framework for modifications to AI/ML based SaMD: "statistical analysis plan"
DAT_CL-2	The manufacturer should specify the inclusion and exclusion criteria for individual data sets.	− There is a specification of technical requirements. − There is a specification of patient attributes that have to be met to include a data set. − There is – if applicable – a specification for the timeframe within data have to be collected	Technical inclusion / exclusion criteria may include for each attribute: − data ranges − data type (numeric (float, integer etc.), ordinal, categorical, String / text, date / time, image / binary) − data formats (e.g. date and number formats) − unit of measure − precision of numbers − attributes values − file formats / types − character encoding − sampling rates	ISO 24028 XAVIER University "Building Explainability and Trust for AI in Healthcare"

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
			– image parameters such as compression, images size, resolution, colour coding, zoom. – language Inclusion / Exclusion criteria of patient data may include the following attributes: – demographic data (age, gender) – physical parameters (height, weight) – diseases – vital parameters – lab parameters – presence of additional tests – case history – special conditions (e.g. patients having heart pacemaker or lung surgery).	
DAT_CL-3	The manufacturer should specify quality control of data.	– There is a list of allowed / expected data sources. – There is a specification of data source requirements. – There is description how invalid input data are identified and excluded.	Data sources may include: – medical devices – in-vitro diagnostic devices – questionnaires – cameras – electronic patient records.	ISO 24028 PSO navigator OECD Privacy Framework

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
		− There is a validation of surveys (justify the selection of the surveys, the time of survey and possibly the method for their assessment, in particular if no standardized survey exists).	Examples for input requirements: − with or without contrast agent (MRT, CT) − number of electrodes (ECG) − voltage (X-Ray, CT) − position of patient. Invalid data may be caused by: − violation of inclusion and exclusion criteria − mistyping e.g.in EMRs, confusion of patients or form fields, misunderstanding of information that has to be entered − different coding of data (It is not uncommon that hospitals apply coding rules differently e.g. for reimbursement reasons) − different units (e.g. kg for babies and pounds for adults). Survey methods may include the type of questions, the types of answers, the decision to have open or closed questions etc.	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
DAT_CL-4	The manufacturer shall analyse the factors that might cause a bias	− There is a list of potential biases	Analysis can be performed (and visualized) by − Directed acyclic graphs − QUADAS-2 (Whiting et al., 2011) and PROBAST (Moons et al. 2019) − DeLong test − FairML (python toolbox) − AI Fairness 360 toolkit − Conditional generative adversarial networks (GANs) Factors causing biases include: − non representative patient population e.g. volunteers, sex, race, age, size, weight, diseases, treatments, social and geographic environment − data collection e.g. types of questionnaires or using channels (e.g. social media) predominantly by certain group − attributes that are irrelevant for the expected output − confusion of correlation and causation − preparation of source data e.g. histopathological slides	ISO 24028 e.g. 10.5 DAISAM

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
			− specific data sources e.g. different type, accuracy − location of data collection e.g. size and type of hospital, rural versus urban − Aggregation that combines data that are not representative for the single populations − "Over-curation" e.g. excluding data from poor quality MRI scans that, however, are common. "Over-curation" also might exclude certain patient profiles	
DAT_CL-5	The manufacturer should specify a distribution of input data that is representative for the target system / population.	− There is a specification of the distribution of relevant patient characteristics.	Characteristics can include: − demographics: age, sex, race − health status, comorbidities − social status, education − motivation to participate in studies. NOTE: Even if all individual data sets meet the specification, still the distribution of data might not be representative and/or cause a bias.	ISO 24028 e.g. 9.8.1 DAISAM
DAT_CL-6	The manufacturer should validate that the test and	− There is a description how it is ensured that data sets that do	Descriptive statistic may include the following:	ISO 24028

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
	training data meet the specified criteria.	not meet the inclusion criteria are actually excluded. – There is a descriptive statistic. – There is a justification that the data are representative for the target population. – There is an analysis of a potential "label leakage".	– calculation of distributions (histograms) – mean / average values – quartiles – joint distribution of features, correlation, etc. Label leakage examples include: – in the sorting (e.g. first the data of healthy persons, then of ill persons) – in the hospital (e.g. if the severe cases originate from just one institution) – in images (e.g. for skin cancer, one must always see a ruler).	
DAT_CL-7	The manufacturer should ensure data protection.	– There is a documented patient data protection policy. – This policy describes the roles (persons, systems) – The is a documented description which role has which type of access (e.g. via user interface, APIs etc.) to which data with which rights (create, delete, change, read) – There should be a documented procedure for data	Data could be derived from machine-to-machine (M2M) communication as well.	GDPR HIPAA ISO 24028 10.6 ISO/IEC 20889:2018(data de-identification)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
		anonymization / pseudonymization. − The policy describes how to decommission data − Data scientists do not have access to protected data. − There is a data protection officer. − There is an ethical approval e.g. for genetic data if legally required		

7.3.2 Data annotation

Table 12: Data annotation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
DAT_AN-1	The manufacturer using "supervised learning" should derive the labels from the intended use and justified this selection.	There is specification for "Label" selection criteria in case of "supervised learning" based machine learning task.		
DAT_AN-2	The manufacturer using "supervised learning" should have a procedure to ensure correct labelling.	− The procedure describes how the ground truth is derived. − The procedure specifies quantitative classification /	If, for example, patients have to be classified as healthy and sick, the manufacturer must derive the criteria specifically for	ISO 13485 clause 4.1

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		segmentation criteria for labelling. – There is a justification of these criteria. – The procedure specifies how and how frequently the correctness of labelling is monitored. – The procedure specifies how to deal with inconsistency of data annotation from multi-annotators. – The procedure specifies the data format and/or syntactic and or standards (e.g. coding system) for annotations – There is a detailed instruction for the task including background information and prototypical examples	the intended use, when a patient is to be classified as healthy and when as sick. DAISAM addresses "label bias"	
DAT_AN-3	The manufacturer should ensure the competency of persons responsible for labelling.	– There is specification for the number of people recruited for "labelling" task. – There is description of the training to be given to persons responsible for 'labelling'.	The results of the monitoring of the labelling can be used to continuously verify the fitness of persons responsible for labelling.	ISO 13485 clause 6.2 and 7.3.2 FDA 21 CFR part 820.25

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– There is specification for the competency level of persons responsible for 'labelling'. – There is a procedure for assessing the success of training success and of the competency for persons responsible for 'labelling'. – There are respective records.		

7.3.3   Data pre-processing

Table 13: Data pre-processing requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
DAT_PR-1	The manufacturer should set a procedure that describes the pre-processing of the data before data is used to train or test the model.	There is documented procedure for data pre-processing: – This procedure describes how the correctness of the interim steps and the final results are assessed through risk-based evaluations. – This procedure specifies how values with various measurement scales or units are detected and processed.	Data pre-processing steps may include the following: – conversion – transformation – aggregation – normalization – format conversion – calculation of feature – conversion of numerical data into categories, etc.	ISO 13485:2016 clauses4.1.6, 7.3.6 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA 21 CFR part 820.70(i)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– This procedure specifies how values are detected and processed that have been collected with various measurement methods. – This procedure specifies how missing values within data sets are detected and processed. – This procedure specifies how unusable data sets are detected and handled as per the data inclusion and exclusion criteria. – This procedure describes how data for training, testing and validation are kept separately. – This procedure describes how new data can be added after initial processing already has been performed (if applicable). – The procedure describes how uniqueness of data is ensured	– statistical analysis e.g. descriptive statistics "Missing value" problem includes "missing at random" and "missing not at random" "Missing value" processing techniques include: – deleting the data set – replacement by the average value of other data sets – new value "missing" (for categorical values), etc. "Outliers" processing techniques include: – deleting the data set – correcting the value – setting the value to a set value (min/max), etc. Examples of unusable datasets may include: – X-rays of poor quality as specified in the technical exclusion criteria or patients/persons who do not meet the patient inclusion criteria. etc.	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			– Uniqueness of data means for example that data are not imported accidentally twice.	
DAT_PR-2	The manufacturer shall analyse and mitigate all risks caused by data processing	– There is a list of factors that can cause distortion and perturbation of data.	Examples for factors causing distortion and perturbation of data are – Rounding errors – Compression, decompression – Noise reduction, filtering – Normalization, transformation, – Resampling – Dealing with outliers, missing values, handling of artefacts	AI4H-DAISAM

7.3.4 Documentation and version control

Table 14: Documentation and version control requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
DOC_VC-1	The manufacturer should describe and control all data processing steps.	– There is a list of data sources.	The description of data sources might include: – location (e.g. clinic)	ISO 24028 9.8.2.2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− There is a document describing all data processing steps mentioned in the previous chapter. − There is a specification of rules for data inclusion and exclusion. − There is a rationale if additional data have been excluded or if data have been kept despite meeting the specification. − The document describes how all data can be traced back to its source. − The document describes how the validity of personnel operation is ensured. − The document describes how compliance with the requirements in chapters **Error! Reference source not found.** to **Error! Reference source not found.** is verified	− capture device. The procedure might specify conventions for − file formats and types − file names − character encoding Means to understand and reproduce the data processing and to prove compliance are − Audit logs − Intermediary data sets − File name conventions − Application of version control − Regression testing with sample data	
DOC_VC-2	The manufacturer should document all software for data processing.	− There is a list of all software applications. − All applications are clearly identified.	Means to identify a software are: − manufacturer − name of software	ISO 13485 clause 4.1.6, 4.2.4 and 7.5.6 FDA 21 CFR part 820.70(i)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− It is identifiable if the software is off-the shelf or individually developed.	− version of software.	
DOC_VC-3	The manufacturer should put all software under version control.	− There is a policy (e.g. SOP) specifying the configuration and version control process. − There are records demonstrating that the software actually is under version control. − The software libraries and frameworks are identified and under version control.		IEC 62304 clause 8 FDA guidance on software validation e.g. chapter 5.2.1
DOC_VC-4	The manufacturer should put all training, test and validation data under version control	− The version of data is aligned with corresponding software versions (software for processing and product)		ISO 13485:2016 4.2.5
DOC_VC-5	The manufacturer shall protect all data and code from loss and unwanted changes	− There is a documented procedure for backups and restoring − There are backup records		ISO 13485:2016 4.2.5

7.4 Model development requirements

7.4.1 Model preparation

Table 15: Model preparation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
MD_PRP-1	The manufacturer should deliberately select the features for training.	− There is a list of features. − There is a rationale as to why a feature is taken into account. − There is an analysis of feature dependencies	Dependencies can be visualized e.g. with a directed Acyclic Graph (DAG).	ISO 24028 9.8.2.2
MD_PRP-2	The manufacturer should deliberately divide the data into training, validation and test data.	− There is justification for the ratio of training, validation and test data. − There is a documented stratification for dividing up the data in to training, validation and test data. − There is documentation that reveals how multiple data sets for an object are in the same "bucket" (training, validation and test data). − There is a justification if data are not distributed at random.	E.g. for data with rare features or labels, it may be necessary to distribute the data not just at random. Example for an object can be a CT scan. The images of one series should not be distributed into the three different "buckets". The splitting strategy for time series data must ensure correct chronological order	ISO 24028 9.8.2.1 DAISAM

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
MD_PRP-3	The manufacturer should document how it ensures that the development team has no access to the test data.	– There is a role-based policy for data access. – There is a description how the development team is prevented from gaining access to test data.		

7.4.2 Model training

Table 16: Model training requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
MD_TR-1	The manufacturer should document model specific data processing.	– There is a document that describes which feature has been recorded specifically for a model or technology.	Examples of this are normalization, selection of class labels (e.g. 0 or 1), selection of column names and distribution of categorical values over multiple columns.	ISO 13485 clause 4.1 FDA 21 CFR part 820.70(i)
MD_TR-2	If there are several quality metrics, the manufacturer should document the quality metrics for the model to which it wants to optimize the model and justified it based on the intended use.	– There are one or more quality metrics identified and respective target values specified. – There is a documented rationale how these quality		

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		metrics relate to the intended use.		
MD_TR-3	The manufacturer should avoid over-fitting.	– There is a policy forbidding the use of test data to optimize the model (only training and validation data may be used).	Visualization (e.g. learning curves) might be helpful for justification and to illustrate the impact of hyperparameter and epochs on quality metrics.	ISO 24028 9.8.2.23
MD_TR-4	The manufacturer should verify that the training actually trains the model	– There is a documentation revealing that the training process improves the model's performance	There is a graph that shows how the loss gets smaller with increasing iterations / epochs.	

7.4.3 Model evaluation

Table 17: Model evaluation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
MD_EV-1	The manufacturer should plan the model evaluation	– There is an evaluation plan. – The plan specifies the evaluation activities, the roles involved and the milestones at which these activities have to be performed.	– The evaluation plan can include activities prior and after product release. The latter activities can be part of the post-market surveillance plan. – The evaluation can include activities in a controlled environment, in closely	ISO 13485 chapters 7.3.2, 7.3.6 and 7.3.7 ISO 14971:2019 chapter 10.

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
			monitored real-world settings and every local site.	
MD_EV-2	The manufacturer should gain an understanding how the machine made a decision to evaluate the correctness and robustness of the model.	− There is a validation specification and validation results for the evaluation of the model with validation data set. − There is a test specification and test results for the final evaluation of the model with new test data. − There are documented values for specified quality metrics. − There may be an analysis of datasets that have exhibited good model performance versus datasets that have performed badly. − For individual data sets there may be an evaluation of the feature that the model particularly determined in the decision. − There may be an analysis/visualization of the dependency (strength, direction) of the prediction of the feature values.	− A residual analysis in which the errors are listed via the feature values. − For classification tasks, the model is particularly insecure with probabilities around 0.5. − This is referred to as "Counterfactuals". This, however, depends on the ML method and cannot be demanded as a general best practice. − Approaches include LIME (Local Interpretable Model-agnostic Explanations), Beta (Black Box Explanations through Transparent Approximations), LRP (Layer-wise Relevance Propagation) and Feature Summary Statistics (incl. Feature Importance and Feature Interaction). This, however, depends on the ML method and cannot be demanded as a general best practice. − Examples of Sharpley-Values, ICE-Plots, Partial Dependency Plots (PDP). This, however, depends on the ML method and	MDR (2017/745) Annex I (17), Annex II (6.1) IEC 62304 clauses 5.5ff. ISO 13485 clauses 7.3.4 ff. XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare" XAVIER University "Building Explainability and Trust for AI in Healthcare" DIN SPECT 2 ISO 24028 10.2 and 10.3

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
		– There may be a synthetization of data sets that activate the model particularly strong. – There may be an approximation of the model using a simplified surrogate model.	cannot be demanded as a general best practice. – Examples of synthetization can be found here http://yosinski.com/deepvis. This, however, depends on the ML method and cannot be demanded as a general best practice. – A manufacturer using synthesized data may argue why this data mimic the actual data respectively why they are suitable to assess the robustness of the model. – A decision tree is an example for a surrogate model. This, however, depends on the ML method and cannot be demanded as a general best practice. – Cross-validation helps to estimate the over fitting	
MD_EV-3	The manufacturer should justify the selection of the model based on its performance on a representative dataset.	– There is a documentation of various models that have been compared. – There is a comparison of these models (architectures). – The comparison includes quality metrics.	Example for quality metrics: see above.	ISO 14971:2019 XAVIER University "Building Explainability and Trust for AI in Healthcare" DIN SPECT 2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
		– There are clearly designed, representative datasets and model performance on those datasets is shown to be adequate following an assessment criterion e.g. an acceptable risk-benefit-ratio. – There is a risk-benefit assessment that discusses interpretability, performance (e.g. quality metrics, efficiency) and robustness.		

7.4.4   Model documentation

Table 18: Model documentation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
MD_DC-1	The manufacturer should document the model.	– There is a documentation of the model (architecture). – There is a documentation of the selected hyperparameters. – There is a documentation of used software libraries and frameworks (also SOUPs).	Ways to document models are the 'model card / sheet' that includes: – model version – assumptions, constraints, dependencies on the algorithm used	ISO 13485:2016 clauses 4.2.3, 4.2.5, 7.3.6 XAVIER University "Building Explainability and Trust for AI in Healthcare"

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
		– There is a documentation of the quality metrics and of the evaluation results e.g. of performance and robustness as specified in Table 17: Model evaluation requirements. – There is a documentation of data the model has been trained on. – There is a documentation of potential problems (e.g. biases) and limitations.	– current performance figures – expected/ optimal performance – major risk conditions. ML models included – linear Regression – logistic Regression – k-nearest neighbours – decision Trees – random Forest – Gradient Boosting Machines – XGBoost – Support Vector Machines (SVM) – Neural Network – k means clustering – hierarchical clustering – Neural Network including Convolutional Neural Network (CNN), Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs) – A-priori algorithm	IEC 62304 on SOUP e.g. clause 8.1.2 FDA OTS guidance ISO 14971:2019

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standards / Regulations applicable
			– Eclat algorithm – Stacked Auto-Encoders – Deep Boltzmann Machine (DBM) – Deep Belief Networks (DBN), etc.	

MD_DC-2	The manufacturer should apply version and configuration control to development artefacts.	– There is a SOP for document respectively version and configuration control.
		– The following artifacts are (additionally to software code and libraries) under version control:
		  o configuration files, hyperparameters
		  o test and evaluation results (including quality metrics)
		  o software libraries and frameworks.
			E.g. trained models can be serialized.	ISO 13485 clauses 7.3.10, 7.5.9.1
				FDA guidance on software validation e.g. 5.2.1
				IEC 62304

7.5 Product development requirements

7.5.1 Software development

Table 19: Software development requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
SFTW-3	The manufacturer should perform and document the required activities pursuant to IEC 62304.	– There is software development plan. – If the model is implemented in another programming language or for another runtime environment, the plan defines which activities of model development have to be repeated. – There is a verification plan that requires software system tests. – The software safety class (alternatively Level of Concern) is determined. – There is a software requirement specification (SRS). – The SRS specifies user interface related requirements. – There is a documented software architecture.	– Adhere to the normal best practices such as adherence to coding guidelines. – Review of code by code-reviews using defined criteria. – Testing to code with unit tests with a defined coverage, etc.	IEC 62304 IEC 82304 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA guidance on software validation FDA OTS guidance ISO 24028 e.g. 10.10

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
SFTW-4	The manufacturer should perform software unit, integration and system tests.	– There are unit-, integration and system tests results. – There are coverage reports. – There is a documented strategy for black box testing. – The tests cover all software / product requirements (including non-functional requirements). – The tests verify risk mitigation measures are effective. – Tests verify that the system safely manages unseen security attacks. – There is a description of tested software version, test data, test environment (e.g. hardware), tester and evaluation of test results. – After changes to the software the tests are repeated unless the manufacturer can	There are specific testing strategies for testing AI-based systems as described in the syllabus of the Korean software testing and qualifications board.(KSTQB & CSTQB Certified Tester AI Testing (CTFL-AIT) (http://www.kstqb.org/eng/sw/sw3_6.asp)) To simulate unseen attacks a test data generator respectively Fuzz tests might be used. The software / product requirements typically include: – performance – functionality e.g. meeting the quality metrics, dealing with invalid data (including warnings) – portability (see testing on target hardware) – interoperability – IT security.	MDR Annex I e.g. 17.1 IEC 62304 5.5-5.7 XAVIER University "Building Explainability and Trust for AI in Healthcare" ISO 2911-4 (testing techniques) DIN SPECT 2 FDA guidance on software validation ISO 24028 e.g. 10.10 Annex C- IT security Guidelines

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		provide a rationale for skipping test activities. – The tests are reproducible.		
SFTW-5	The manufacturer should test software on the target hardware.	– The test hardware is specified. – The test hardware is representative for the target hardware. – The tests verify whether the specified performance requirements are met.	Performance may include: – response times – resource consumption. Hardware may include – browser – mobile device, etc.	MDR (2017/745) Annex II 6.1 FDA guidance on software validation e.g. 5.2.5 and 5.2.6
SFTW-6	The manufacturer should identify and verify all SOUP /OTS components.	– There is a list of all SOUP / OTS components. – Each SOUP / OTS component is uniquely identified. – Each SOUP / OTS component is under version control. – The requirements for each SOUP / OTS component are specified. – The is a documented trace between these requirements and respective tests.	Components can be uniquely identified by: – manufacturer – name of component – version of component. – Traces can be documented using ALM tools or tables. Examples for prerequisites are: – hardware (e.g. processor architecture, RAM) – software (e.g. operating system, run-time environments e.g. .NET, browser) – AI acceleration hardware/inference acceleration hardware	IEC 62304 clauses 5.3 and 8.1.2 FDA OTS guidance

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– The prerequisites for each SOUP /OTS component are specified.	Comment: For comparative definitions, similarities and differences of SOUPs, COTS, OTS terms, please refer to https://www.johner-institute.com/articles/software-iec-62304/soup-and-ots/	
SFTW-7	The manufacturer shall validate the software tools	– There is a validation plan for the training functionality of ML library – There are respective validation results – There is a documented rationale that the		IEC 13484:2016 4.1.6

7.5.2 Risk Management

Table 20: Risk Management

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
RSK_MGNT-16	The manufacturer shall assess and mitigate the risks that occur	– There is a specification of functionalities of the chosen	– Input for risk-based tool validation	MDR, IVDR Annex I e.g. section 3. ISO 13485:2016 3.1.6

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	specifically to the chosen ML libraries	ML libraries that are used for training – There is a specification of functionalities of the chosen ML libraries that are used for prediction – There is an analysis of risks of a training function not meeting the specifications – There is an analysis of risks of predict function not meeting the specifications	– Input for risk-based SOUP validation	IEC 62304 5.3.3 ISO 14971:2019
RSK_MGNT-17	The manufacturer shall assess and mitigate the risks that occur specifically to the chosen software architecture	– The risk analysis analyses risk for the most important components at least – The risk analysis analyses risks that are specifically to chosen technologies	– Risks related to client server architecture – Risks related to (de)serialization of data – Risks related to format and protocol conversions – Risks related to multiple API versions and API gateways – Risk related specifically for programming language – Risks related to compiler and compiler settings	
RSK_MGNT-18	The manufacturer shall assess and mitigate risks related to data processing (e.g. during training)	– There is a list of all steps of data processing and annotation.	– Error in format conversion	

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– There is an analysis of errors that can occur for each processing step – There is an analysis of risks arising from these errors	– Errors in detecting and dealing with missing values – Errors in detecting and handling outliers – Errors in unit conversions – Errors in converting numeric in categorical values – Errors due to loss of data – Errors due to confusing data sources – Errors in feature extraction	
RSK_MGNT-19	The manufacturer shall assess the risks related to design transfer.	The risks analysis analyses consequences of porting the software and data to the target system.	The target system includes for example: – Hardware – Operating system – Other software	
RSK_MGNT-20	The manufacturer shall assess the risks caused by the specific selection of data.	– The risk analysis analyses consequences of model bias. – The risk analysis analyses consequences of wrong reference data (e.g. wrong gold standard, wrong comparison)	See. DAT_CL-4	

7.5.3 Accompanying materials

Table 21: Accompanying materials requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
MTR-1	The manufacturer should provide instructions for use.	– There are instructions for use. – The instructions for use clearly identify the version of the product. – There is a procedure specifying how to develop and verify instructions for use. – The document on instructions for use is under version control.	The identification of the product should be achieved by the product's UDI-DI.	MDR (2017/745) Annex I (23.4) FD&C, FDA 21 CFR parts801 and 820.120 ISO 24028 e.g. 10.11.3
MTR-2	The instructions for use should describe the intended purpose and intended use.	– The instructions for use specify the intended medical purpose and medical benefit. – The instructions for use specify the intended patient population including indications, contraindications and if relevant other parameters. – The instructions for use specify the patients / data / use case for which the product may not be used.	The medical purpose and benefit typically are related to diagnosis, treatment, prognosis and monitoring of certain diseases or injuries. The patient population can be characterized by age, gender or accompanying diseases Examples for input data requirements are: – formats – resolutions	MDR (2017/745) Annex I (23.4) 21 CFR part 801 21 CFR part 814.20 XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare" ISO 24028 XAVIER University "Building Explainability and

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– The instructions for use reveal limitations. – The instructions for use specify the requirements of the input data. – The instructions for use specify the intended primary and secondary users pursuant to intended use. – The instructions for use describe the other conditions applicable to the product (e.g. runtime environment, use environment). – The instructions for use describe how to update the product. – The instructions for use of continuous learning systems describe what triggers algorithm updates and how to identify the version of this algorithm. – The instructions for use of continuous learning systems describe how to permit, delay and roll-back algorithm updates.	– value ranges, etc.	Trust for AI in Healthcare" ISO 24028 e.g. 10.11.3

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
MTR-3	The instructions for use should specify the performance of the product.	– The instructions for use specify the quality metrics.	– Examples of quality metrics are specificity, sensitivity, precision.	MDR (2017/745) Annex I (23.4)
MTR-4	The instructions for use should explain the product and its working principle / underlying principle.	– The instructions for use indicate the data with which the model was trained. – The instructions for use describe the model and algorithms. – The instructions for use specify whether the product is further trained during use. – The instructions for use provide information whether and if yes how the system learns over time.		MDR (2017/745) Annex I (23.4)? XAVIER University: Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare TODO: Reference to AI/ML standards
MTR-5	The instructions for use should reveal residual risks.	– The instructions for use list the factors that could have a negative effect on the product's performance. – The instructions explain risks arising from a product not meeting the performance requirements. – The instructions for use list possible ethical problems.	Examples of negative factors are: – patient population deviating from specified population – data not meeting the specified criteria (e.g. formats, value ranges). –	EU MDR (2017/745) Annex 1 23.4 ISO 14971:2019 clause 8 ISO 24028 e.g. 10.11.3
	The instructions for use should further information that is legally required.	– The instructions for use identify the manufacturer.		EU-MDR (2017/745) Annex 1 23.4

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– The instructions for use lists channels for posing questions. – The instructions for use contain references to licensing rights. – The instructions for use contain the URL under which the most current versions of the instruction of use can be found.		EU-Regulation 207/2012

7.6 Product validation requirements

7.6.1 Usability validation

Table 22: Usability validation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
U_VLD-1	The manufacturer should identify risk arising from a lack of usability.	– The risk management file lists risks that arise from misunderstanding, overlooking or ignoring the product's visual output. – The risk management file lists risks that arise from	The product's visual output includes: – results e.g. treatment recommendations, diagnosis – limitations of the system	ISO 14971:2019: 5.2 IEC 62366-1 clause 4.1 XAVIER University "Building Explainability and Trust for AI in Healthcare"

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		users blindly trusting or mistrusting the product.	– warnings e.g. whether preconditions are met – trustworthiness of results – reports, printouts. – The manufacturer could evaluate how obvious the systems output is before users become suspicious.	FDA HFE guidance ISO 24028 9.7 FDA proposed regulatory framework for modifications to AI/ML based SaMD chapter 4
U_VLD-2	The manufacturer should assess whether the users understand the instructions for use.	– The risk management file lists the risks that have to be mitigated by instructing users e.g. by training or accompanying materials. – The plan of the summative evaluation describes how the effectiveness of these measures is validated. – The usability evaluation report reveals whether the instructions for use are adequate to mitigate risks.		IEC 62366-1 (instructions for use are considered to be part of accompanying documentation that is considered to be part of the user interface) FDA HFE guidance

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
U_VLD-3	The manufacturer should evaluate all safety relevant use scenarios.	– There is a list of use scenarios. – There is an assessment of safety relevance for each use scenario. – The use scenarios included in the summative evaluation cover all safety relevant use scenarios. – The summative evaluation evaluates the effectiveness cover all risk mitigation measure.		IEC 62366-1 clause 5.4 ff.
U_VLD-4	The manufacturer should define and specify the usability metrics for (a) understandability, (b) learnability and (c) operability of AIMD	Specifications for following metrics – Product description completeness – Function understand-ability – Input and Outputs understand-ability – Ease of learning product functions – User documentation effectiveness – Operational error recoverability – Customizability – Physical accessibility – other	– What proportion of functions are understood by reading the product description /manual? – What proportion of interface functions are understandable? – How long does the user take to learn to use a function? – How easily the user can understand the messages from software system? – How easily the user can recover from his/her worse situation?	ISO/IEC 9126-2 (Part-2: External Metrics)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
			– How easily the user can customize operation procedures for his/her convenience? – What proportion of functions are accessible to users with physical impairments	
U_VLD-5	The manufacturer should define and specify the 'quality in use'-metrics to measure the extent to which AIMD meets the needs of target users to achieve specified goals of effectiveness, productivity, and satisfaction in a specified context of use.	Specifications for following metrics – Task effectiveness – Task completion – Error frequency – Task time – User wait time – Frequency of use of system help features – User satisfaction scale – Other	– What proportion of the task is completed correctly by the user? – What is the frequency of errors encountered by the user? – How long does the user take to complete a task? – What proportion of the time do users spend waiting for the system to respond?	ISO/IEC 9126-4 (Part-4: Quality in use-metrics)

7.6.2 Clinical evaluation

Table 23: Clinical evaluation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
CLC_EV-1	The manufacturer should assess whether the promised medical benefit is achieved with the quality parameters.	– The clinical evaluation contains the medical benefits the manufacturer claims. – The clinical evaluation lists the data (sources) that have been evaluated and that support and that contradict the hypothesis, that the benefits have been achieved. – If the data have been collected from other products, than the clinical evaluation discusses the clinical and technical equivalence of the other products. – The clinical evaluation evaluates the impact of quality parameters on the achievement of the medical benefit.	– The data are typically clinical data. – The technical equivalence has to consider the software algorithms.	EU MDR (2017/745) Article 61 and Annex XIV and XV MEDDEV 2.7/1 rev. 4 XAVIER University "Building Explainability and Trust for AI in Healthcare" FDA 21 CFR part 820.30(g)
CLC_EV-2	The manufacturer should assess whether the promised medical benefit is achieved is consistent with the state of the art.	– The clinical evaluation lists alternative methods, technologies or procedures.	Alternative approaches include: – a non- continuously learning model in comparison with a	EU MDR (2017/745) Article 61 and Annex XIV and XV MEDDEV 2.7/1 rev. 4 ISO 14971:2019 4.2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– The clinical evaluation compares the risks and benefits of these alternatives.	continuously learning model – classic algorithm in comparison with a machine learning model.	

7.7 Product release requirements

Table 24: Product release requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
PDT_RLS-1	The manufacturer should verify the completeness of documentation.	– There is a risk management report concluding that all risk management related activities have been performed according to risk management plan and that residual risks are acceptable. – There is a usability evaluation report concluding that all activities to formative and summative evaluation plan have been performed. – There is a documentation of the model.	The documentation of the model should at least cover all aspects that have been mention in chapter "instructions of use".	MDR (2017/745) Annexes I and II ISO 13485 e.g. 7.3.5 FDA 21 CFR part 820.30(e)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
PDT_RLS-2	If the manufacturer of a continuous learning system plans to market its product in the US market it should compile the respective documentation.	– There is a "Software as a Medical Device Pre-Specifications "(SPS) that anticipates changes to the product. – There is an "Algorithm Change Protocol (ACP)"that specifies how these changes for systems will be performed. Note: Manufacturer may further clarify with authorities if SPS / ACP is desired for submission		FDA: Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)- Based Software as a Medical Device (SaMD)

8 Post-market requirements

8.1 Production, distribution & installation requirements

Table 25: Production, distribution & installation requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
PDT_INST-1	The manufacturer should apply version- and configuration control.	– There is a SOP or work instruction that specifies how the manufacturer identifies artefacts and how it ensures how the correct	– The bill of material also contains all SOUP/OTS Software.	IEC 62304 clause 8 FDA Cybersecurity Guidance ISO 13485:7.5.8

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– artefacts in the respective version are delivered. – Version and configuration control apply to the software as well to accompanying materials such as instructions for installation and use. – There is a bill of materials. – There is a unique identification (ID) of the product.	– In EU and in the US, there is typically the need for a UID-DI and UDI-PI. Comment: For comparative definitions, similarities and differences of SOUPs, COTS, OTS terms, please refer to https://www.johner-institute.com/articles/software-iec-62304/soup-and-ots/	FDA Guidance on Software Validation Annex C- Cyber-security
PDT_INST-2	The manufacturer should ensure the design transfer.	– There is a SOP or work instruction that specifies how the persons responsible for installation know which is the most current version and how mistakes in installation can be ruled out. – There are instructions for installation, update and decommissioning. – These instructions specify the runtime environment. – There instructions specify how the correct installation can be verified.	The specification of the production runtime environment can include: – hardware (CPU, RAM) – monitors, displays (size, resolution, orientation) – operating system.	ISO 13485 clause 7.3.8 21 CFR 820.30(h) 21 CFR 820.170
PDT_INST-3	The manufacturer should ensure effective and efficient	– There is a SOP covering customer communication		ISO 13485 clauses 5.2 and 7.2

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	communication with operators and users, including any security-related requirements that are the responsibility of the operators / users. The manufacturer also needs a mechanism to communicate security issues with their customers (e.g. a new vulnerability was discovered and the customer should take adequate steps to minimize potential harm until the manufacturer can fix the problem.)	including handling of customer complaints. – There is a website that contains information about latest product releases and news related to security vulnerabilities. – The website provides the means to download the software. – The instructions for use reference this website. – The instructions for use and the website reveal contact information e.g. e-mail, phone number, and/or a contact form.		MDR (2017/745) Article 10(j) MDR (2017/745) Annex I (23.1) Annex C- IT security Guidelines

8.2 Post-market surveillance requirements

Table 26: Post-market surveillance requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
PST_MRK-1	When determining threshold values the manufacturer should analyse how the application of	– There is an analysis, whether feedback loops can influence input values.	– Example for feedback loop: An algorithm provides prognoses.	MDR (2017/745) Annex III (1.1)

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
	the product might impact feature (input values).	– There is an analysis, whether self-fulfilling prophecies can influence input values. – There is a specification of threshold values in the post-market surveillance plan.	Therefore, the physician will treat the patients better or earlier. – Example for self-fulfilling prophecies: an algorithm for predicting date and location of crimes will cause a higher surveillance by police. This will cause an increased number of detected crimes.	
PST_MRK-2	The manufacturer should compile a Post-Market Surveillance Plan.	– There is a SOP specifying how to compile post-market surveillance plans. – There is a post-market surveillance plan specifically for the product. – The plan lists all relevant data sources to be monitored. – These sources include information from SOUP manufacturers (also of ML libraries) and also includes security disclosures by those vendors – The plan describes for each data source how, how often and by whom data are collected.	– "By whom" not only persons / roles, but also systems can be listed Examples for data sources are: – results from leading ML conferences – scientific literature – customer communication (e.g. complaints) – IT security databases – bug reports and release notes for SOUP / OTS – databases of authorities (e.g. FDA) – actual input values (features) for continuous	MDR (2017/745) Article 10(i) MDR (2017/745) Article 83 MDR Annex III (1.1) FD&C act 522 21 CFR part 822 IEC 62304 7.1.3 XAVIER: "Perspectives and Good Practices for AI and Continuously Learning Systems in Healthcare" ISO 24028 DIN SPECT 2 FDA proposed regulatory framework for modifications to

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− The plan specifies how data has to be analysed. − The plan requires that quality metrics such as sensitivity and specificity are monitored. − The plan specifies the data to be collected to be able to analyse whether the data in the field is consistent with the expected data or training data. − The plan requires to collect and analyse data to assess how the use of the system changes over time. − The plan for continuous learning systems specifies whether and if how often which data sets have to be retested after algorithm updates. − The plan for continuous learning systems specifies how and how frequently changes in algorithm updates are assessed. − The plan lists threshold values that trigger actions.	training and or usage of the product − audit-logs. Examples for additional quality metrics see above. Also, the variance of these quality metrics over time might be a quality metric (This allows visualization or quantification in particular for non-normally distributed data over the comparison of histograms or core density estimations). The post-market plan should consider shifts such as − Concept drift − Distribution shifts (labels) − Distribution shifts (feature) Actions include update of risk analysis and re-evaluation of risk-benefit analysis, re-training of algorithm, product recall, implementation of better risk mitigation measures.	AI/ML based SaMD chapter IV Annex C- IT security Guidelines

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		– The threshold values include quality metrics. – These threshold values include features. – The plan specifies the frequency and content of compiling post-market surveillance reports. – The plan is approved.		
PST_MRK-3	The manufacturer should perform post-market surveillance and compile reports, both according to the post-market surveillance plan.	– There is a post-market surveillance report for each product respectively product type. – The post-market surveillance reports clearly identify the respective products via its UDI. – The post-market surveillance reports identify the post-market data and conclude whether activities are required.		MDR (2017/745) Article 85 f. FDA proposed regulatory framework for modifications to AI/ML based SaMD chapter IV
PST_MRK-4	The manufacturer should establish a post-market risk management system.	– There is a specification how, how often and by whom the state of the art is monitored and re-assessed. – The state-of-the-art assessment takes latest algorithms for machine	– It is possible to combine post-market risk management and post-market surveillance. – The interpretability includes transparency and explainability.	ISO 14971 clause 10

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− learning and for improving interpretability into account. − The state-of-the-art assessment takes alternatives for the "ground-truth" respectively the gold standard. − There is a specification how, how often and by whom post-market data are evaluated for new or changed hazards, hazardous situations, and risks. − The post-market risk analysis searches for (adverse) behavioural changes or (foreseeable) misuse. − For products that have been placed on the market for more than one-year post-market risk management activities are documented.	− The foreseeable misuse may include radiologists that rely on the software and don't look at the images anymore, so they overlook finding. − The foreseeable misuse can include users or operators not updating the software or using the product after communicated end of life.	
PST_MRK-5	The manufacturer, must assess the design change before deciding whether notified bodies respectively authorities have to be informed.	− For products marketed in the US there is an Algorithm Change Protocol (ACP) and a "SaMD Pre-Specifications" (SPS). − There is a description of design changes.	Descriptions of design changes take into account changes to: − intended use − ML architecture − software architecture	MDR (2017/745) Article 87 ff. ISO 13485 clause 7.3.9 21 CFR part 820.30(i) FDA's "Proposed Regulatory Framework for Modifications to

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− There is an impact analysis for these design changes.	− use of 3rd party libraries (SOUP, OTS) − programming language − user Interface including warning − data interfaces.	Artificial Intelligence / Machine Learning (AI/ML) Based Software as Medical Device

8.3 Decommissioning requirements

Table 27: Decommissioning requirements

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
DE_CMSN-1	The manufacturer should establish a plan before decommissioning the medical device.	The plan describes − information of users and operators − disposal of product − archiving of product and data (e.g. training, test, validation data), software, documentation, considering security and privacy concerns	Disposal can include: − putting product into trash − de-installation − sending back to manufacturer − logging-off − "de-registration" − confirmation of disposal.	ISO 24028
DE_CMSN-2	The manufacturer should analyse risks of decommissioning.	The risk analysis assesses:	− Disturbance of workflows.	MDR Annex I, 3. ISO 14971:2019 chapter 10 in

REQ. ID	Requirement(s)	Checklist item(s)	Checklist examples and comments	Standard(s) / Regulation(s) applicable
		− risks for patients due to a product that is no longer available. − risks due to negative impact on other systems.	− Interoperability problems.	combination with 3.8 and 3.12 ISO 24028

Annex A
AI/ML related activities in the product life cycle

To facilitate continual product improvement in an iterative and adaptive manner with conformance to appropriate standards and regulations, it becomes a good practice for any regulatory framework to establish a system that can ensure transparency and accountability of all the life cycle processes involved in AI4MD development shown in Figure A.1. A brief rationale is provided in this section on the need for a product development lifecycle process oriented approach that forms the basis of the proposed regulatory requirements guidelines
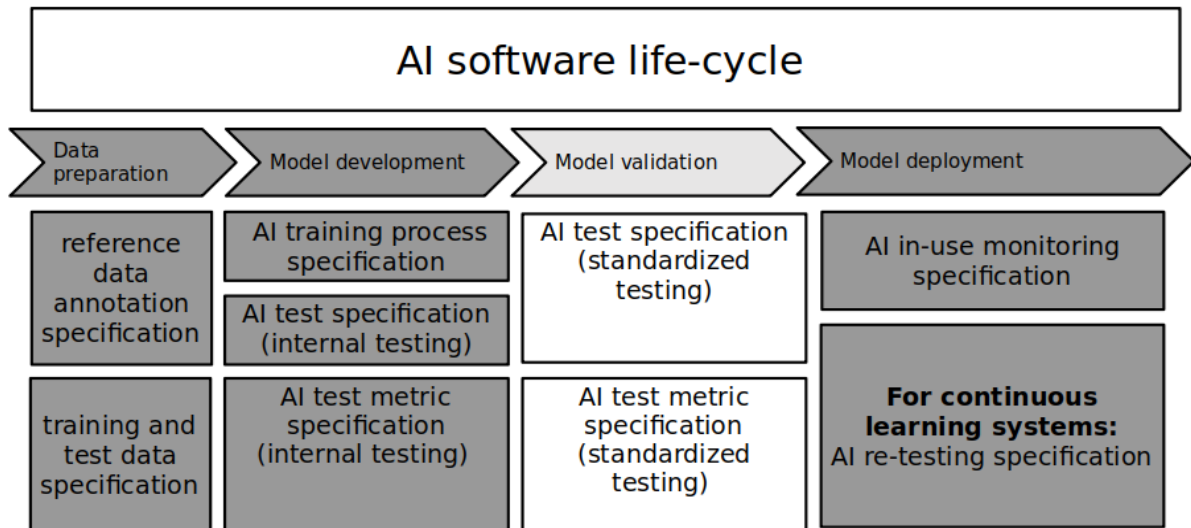
Figure A.1: AI Software life-cycle diagram
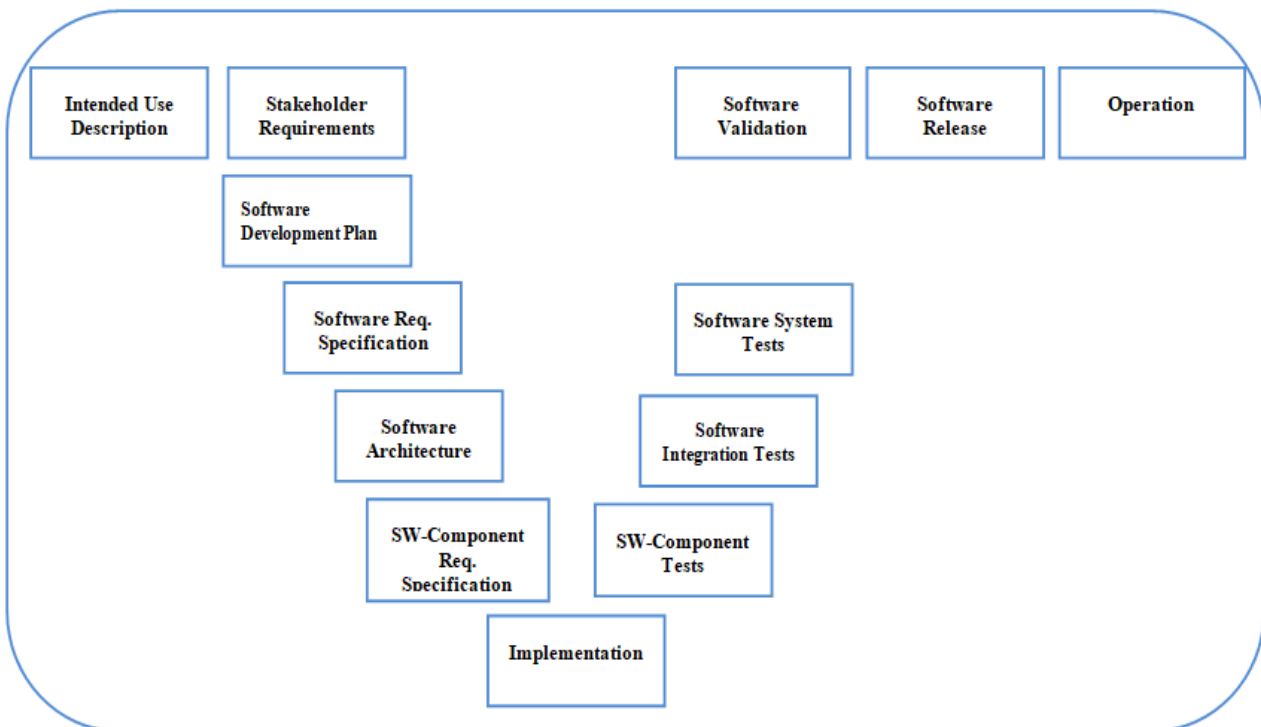
Figure A.2: Product development life-cycle process (V-model)

Figure A.2 shows the V-model, which is widely accepted as a good practice product development lifecycle model in software engineering practice.

– A V- model based regulatory roadmap is proposed with an aim to maximize the completeness and coverage of various regulatory needs / aspects across the AI-MD life cycle processes - requirements, design, development, testing, deployment, maintenance, etc.

– The V- model supported by the principles of transparency and real-world performance monitoring, conformance assessments can be performed to measure and trace the compliance / deviation of in-house processes with standardized regulatory assessment procedures

– Apart from compliance verification, V-model gives thrust to software process improvement and supports integration of best practice for process improvement to achieve improved software quality, performance, safety, and effectiveness of medical device.

Annex B
Priority assessment scheme

B.1   Regulatory guidelines: requirements checklist

A regulatory requirement assessment checklist is proposed as a standard assessment and reporting tool to aid regulatory auditing/review process. Checklist enlists an orderly set of verification and validation procedures on how to conduct a comprehensive review covering all relevant aspects of the quality assurance pipeline.

The quality criteria for a checklist item include the following:
–   It is atomic (not a combination)

–   It can be checked within seconds or maximum a few minutes

–   The result is binary i.e. either 'Yes' or 'No'

–   It clearly specifies the necessary evidence

–   It is understandable and verifiable also for non-experts

–   It has to match / prove the requirement

NOTE: The checklist contained in this document is an aide-memoire. It cannot substitute for adequate training of people who will use the checklist and who therefore must understand the expressed requirements in context. Regulators, manufacturers, and other organizations adopting the checklist should ensure that the personnel designated to use it have the requisite educational background, professional experience, and specific training required to use it properly.

B.2   Requirements Checklist: Priority Assessment Scheme

B.2.1   About priority score

All of the requirements listed in this document are necessary, if not sufficient in all circumstances for manufacturing every type of AI health application. That said, it may not be possible 1) to meet all requirements when building a QMS or 2) to apply them all when auditing manufacturing processes or evaluating products. In such circumstance, one could decide that some requirements are more important than others, e.g., based on the potential for harm relative to the expected benefit to patients, and thus should be addressed first. Again, priority may depend on the type of AI health application and/or other considerations. The failure to meet the most important requirements may be considered to be major deficiencies; other requirements may be considered lesser deficiencies.

To develop a priority score, it is necessary to
1.   establish a priority scale (and to define each scale point),

2.   to develop in operating detail criteria for differentiating one scale point from another, and

3.   to decide the appropriate scale point for each requirement.

While each regulator could decide these matters for itself, to assist regulators, this document provides the following guidance with respect to these matters. Additionally, users of priority scores need to ensure that they are implemented reliably, both by a given person and among people. Ensuring such inter-reliability may require specific educational background or professional experience, development of an implementation tool, and training in its use, among other methods. Further, through appropriate data collection and analysis, regulators could assess the validity of assigned priority scores based on examining them in relation to patient outcomes, and, if necessary, could

accordingly adjust scoring criteria, implementation methods, etc. Such application considerations are beyond the scope of this document.

B.2.2   Priority score: purpose

The priority score was developed to suggest to regulators, auditors, and QMS personnel which checklist items should be given highest priority when resources are not sufficient to address them all simultaneously or when only limited time is available in which to complete an audit. If a manufacture is failing to meet or to comply with requirements, it should take appropriate action to resolve underlying problems. If there are many such failures, the priority score may help to decide the order in which they should be addressed.

B.2.3   Priority score: decision anchor

The importance of a checklist item is risk-based, i.e., it depends upon specific consequences of not meeting or not complying with the requirement. These consequences are
1.   ultimately, patient safety, i.e., the risk of harm to patients exposed to the product (and, when applicable, the risk of harm to users of the product, bystanders, and other involved persons) and

2.   proximally, failure to meet established product specifications (which in turn has the potential to impact adversely patient safety).

In other words, failure to meet an important requirement can be expected to result in
1.   products that do not meet one or more product specifications and

2.   if such products were to be used would be expected to cause serious harm to patients.

NOTE – It is possible that a product meets all product specifications and can still causes serious harm to patients. This is a different problem; one that requires appropriate clinical testing or monitoring, and sound decision-making based on appropriate weighing or risks and benefits. Such decisions may include changing product specification and/or indications for use of the product. It is possible that a manufacturer meets all process requirements but still produces products that do not reliably meet product specifications. This is a manufacturing quality management system problem; one to be resolved through appropriate investigation and subsequent action.

B.2.4   Priority scale

We established the following 3-point importance scale. This scale is independent of whether or not a requirement is currently mandated by a regulator in at least one jurisdiction. In other words, the scale may differentiate the importance of different regulatory requirements. The checklist of requirements included in this document indicates in which regulations a requirement may be found, if any, i.e., the source of each listed requirement.

B.2.5   Priority criteria

We established the following operational criteria to assign each listed requirement to a priority scale point.
1.   **High importance:** Not fulfilling this requirement can be expected to cause serious patient harm or a major non-compliance in audits/inspections.

2.   **Intermediate importance:** Not fulfilling this requirement can be expected to cause severe patient harm or a minor non-compliance.

3.   **Less important:** It is not expected that not fulfilling this requirement will lead to patient harm nor to a non-compliance over the product entire lifespan.

B.2.6   Priority scores for checklist requirements

Using the above-described criteria, manufactures can assign a priority score to each listed requirement, arriving at such score by consensus. The resultant priority scores can be included in the table of requirements before submitting it to the regulators, auditors, and QMS personnel

Annex C
Relationship to other guidelines and standards

The proposed guidelines were formulated based on a critical review of existing global regulations and standards for AI related technologies in medical applications. The critical review included identifying the gaps of existing regulatory requirements assessments methods and incorporating a quality risk management approach with necessary monitoring and control parameters for improved safety and efficiency of AI-MDs. A detailed list of regulatory references considered towards the formulation of the proposed guidelines are included here.

C.1   IMDRF essential principles

IMDRF- Essential principles provide broad, high-level, criteria for design, production, and postproduction throughout the lifecycle of all medical devices and IVD medical devices, ensuring their safety and performance

IMDRF Essential Principles (EPs) were evaluated to cover aspects considered applicable to the regulation of SaMDs. Main IMDRF references include the following:
1.   "Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices", IMDRF Good Regulatory Review Practices Group, IMDRF GRRP WG/N47 FINAL, 31 October 2018 (http://www.IMDRF.org/docs/IMDRF/final/technical/IMDRF-tech-181031-grrp-essential-principles-n47.pdf)

2.   Table for use in mapping IMDRF Essential Principles (31 October 2018) to controls for Artificial Intelligence and Machine Learning Algorithms utilized in Medical Technology

The scope of EPs applicable to AI-MDs cover the following:
A.   Safety and Performance of Medical Devices – General Essential Principles

B.   IMDRF Essential Principles Applicable to all Medical Devices and IVD Medical Devices

–   General

–   Clinical Evaluation

–   Medical Devices and IVD Medical Devices that Incorporate Software or are Software as a Medical Device

–   Medical Devices and IVD Medical Devices with a Diagnostic or Measuring Function

–   Labelling

–   Protection against the Risks posed by Medical Devices and IVD Medical Devices intended by the Manufacturer for use by Lay Users

C.   Essential Principles Applicable to IVD Medical Devices

–   Performance characteristics

Details on the Essential Principles and their mapping to AI4 concepts are given below.

NOTE: EP#: refers to original section numbers in the document- "Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices", IMDRF Good Regulatory Review Practices Group, IMDRF GRRP WG/N47 FINAL, 31 October 2018.

Table C.1: IMDRF EP 5.1 – General

EP #	EP requirements	EP key concepts
5.1.1	Medical devices and IVD medical devices should achieve the performance intended by their manufacturer and should be designed and manufactured in such a way that, during intended conditions of use, they are suitable for their intended purpose. They should be safe and perform as intended, should have risks that are acceptable when weighed against the benefits to the patient, and should not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons.	Performance; Intended conditions of use; Safety; Perform as intended; Acceptable risks; Patient benefits; Health
5.1.2	Manufacturers should establish, implement, document and maintain a risk management system to ensure the ongoing quality, safety and performance of the medical device and IVD medical device. Risk management should be understood as a continuous iterative process throughout the entire lifecycle of a medical device and IVD medical device, requiring regular systematic updating. In carrying out risk management manufacturers should:	Risk management system; Quality; Safety; Performance; Continuous, iterative risk management; MD life cycle
5.1.2	a) establish and document a risk management plan covering each medical device and IVD medical device;	Risk management plan
5.1.2	b) identify and analyse the known and foreseeable hazards associated with each medical device and IVD medical device;	Identify and analyse hazards
5.1.2	c) estimate and evaluate the risks associated with, and occurring during, the intended use and during reasonably foreseeable misuse;	Risk; Intended use; Foreseeable misuse
5.1.2	d) eliminate or control the risks referred to in point (c) in accordance with the requirements of points 5.1.3 and 5.1.4 below;	Risk elimination; Risk control
5.1.2	e) evaluate the impact of information from the production and postproduction phases, on the overall risk, benefit-risk determination and risk acceptability. This evaluation should include the impact of the presence of previously unrecognized hazards or hazardous situations, the acceptability of the estimated risk(s) arising from a hazardous situation, and changes to the generally acknowledged state of the art.	Continuous, iterative risk management
5.1.2	f) based on the evaluation of the impact of the information referred to in point (e), if necessary, amend control measures in line with the requirements of points 5.1.3 and 5.1.4 below.	Continuous, iterative risk management; Update control measures
5.1.3	Risk control measures adopted by manufacturers for the design and manufacture of the medical device and IVD medical device should conform to safety principles, taking account of the generally acknowledged state of the art. When risk reduction is required, manufacturers should control risks so that the residual risk associated with each hazard as well as the overall residual risk is judged acceptable. In selecting the most appropriate solutions, manufacturers should, in the following order of priority:	Risk control measures; Safety principles compliance; State of the art; Risk control
5.1.3	a) eliminate or appropriately reduce risks through safe design and manufacture;	Safe design

EP #	EP requirements	EP key concepts
5.1.3	b) where appropriate, take adequate protection measures, including alarms if necessary, in relation to risks that cannot be eliminated; and	Alarms; risks that cannot be eliminated
5.1.3	c) provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users.	Alarms; User training
5.1.4	The manufacturer should inform users of any relevant residual risks.	Residual risk information for user
5.1.5	In eliminating or reducing risks related to use, the manufacturer should:	Risk reduction
5.1.5	a) appropriately reduce the risks related to the features of the medical device and IVD medical device and the environment in which the medical device and IVD medical device are intended to be used (e.g. ergonomic/usability features, tolerance to dust and humidity) and	Risk reduction; Intended usage environment
5.1.5	b) give consideration to the technical knowledge, experience, education, training and use environment and, where applicable, the medical and physical conditions of intended users.	Consider user knowledge
5.1.6	The characteristics and performance of a medical device and IVD medical device should not be adversely affected to such a degree that the health or safety of the patient and the user and, where applicable, of other persons are compromised during the expected life of the device, as specified by the manufacturer, when the medical device and IVD medical device is subjected to the stresses which can occur during normal conditions of use and has been properly maintained and calibrated (if applicable) in accordance with the manufacturer's instructions.	Stress resistance; Intended use; Expected life of device
5.1.7	Medical devices and IVD medical devices should be designed, manufactured and packaged in such a way that their characteristics and performance, including the integrity and cleanliness of the product and when used in accordance with the intended use, are not adversely affected by transport and storage (for example, through shock, vibrations, and fluctuations of temperature and humidity), taking account of the instructions and information provided by the manufacturer. The performance, safety, and sterility of the medical device and IVD medical device should be sufficiently maintained throughout any shelf-life specified by the manufacturer.	-
5.1.8	Medical devices and IVD medical devices should have acceptable stability during their shelf-life, during the time of use after being opened (for IVDs, including after being installed in the instrument), and during transportation or dispatch (for IVDs, including samples).	Stability; Shelf life
5.1.9	All known and foreseeable risks, and any undesirable side-effects, should be minimized and be acceptable when weighed against the evaluated benefits arising from the achieved performance of the device during intended conditions of use taking into account the generally acknowledged state of the art.	Risk; Side-effects

Table C.2: IMDRF EP 5.2 – Clinical evaluation

EP #	EP requirements	EP key concepts
5.2.1	Where appropriate and depending on jurisdictional requirements, a clinical evaluation may be required. A clinical evaluation should assess clinical data to establish that a favourable benefit-risk determination exists for the medical device and IVD medical device in the form of one or more of the following: – clinical investigation reports (for IVDs, clinical performance evaluation reports) – published scientific literature/reviews – clinical experience	Clinical evaluation; Benefit-risk determination; Clinical investigation report; Published scientific literature; Clinical experience
5.2.2	Clinical investigations should be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki. These principles protect the rights, safety and well-being of human subjects, which are the most important considerations and shall prevail over interests of science and society. These principles shall be understood, observed, and applied at every step in the clinical investigation. In addition, some countries may have specific regulatory requirements for pre-study protocol review, informed consent, and for IVD medical devices, use of leftover specimens.	Ethical principles; Declaration of Helsinki Rights; Safety; Well-being; Pre-study protocol review; Informed consent; Leftover specimen

Table C.3: IMDRF EP 5.8 – Medical devices and IVD medical devices that incorporate software or are software as a medical device

EP #	EP requirements	EP key concepts
5.8.1	Medical devices and IVD medical devices that incorporate electronic programmable systems, including software, or are software as a medical device, should be designed to ensure accuracy, reliability, precision, safety, and performance in line with their intended use. In the event of a single fault condition, appropriate means should be adopted to eliminate or appropriately reduce consequent risks or impairment of performance.	Electronic programmable systems; Software; Software as a medical device; Accuracy; Reliability; Precision; Safety; Performance; Single fault conditions; Risk reduction
5.8.2	For medical devices and IVD medical devices that incorporate software or are software as a medical device, the software should be developed, manufactured and maintained in accordance with the state of the art taking into account the principles of development life cycle (e.g., rapid development cycles, frequent changes, the cumulative effect of changes), risk management (e.g., changes to system, environment, and data), including information security (e.g., safely implement updates), verification and validation (e.g., change management process).	State of the art; Principles of development life cycle (e.g., rapid development cycles, frequent changes, the cumulative effect of changes); Risk management (e.g., changes to system, environment, and data); Information security (e.g., safely implement updates); Verification; Validation; Change management process
5.8.3	Software that is intended to be used in combination with mobile computing platforms should be designed and developed taking into account the platform itself (e.g. size and contrast ratio of the screen,	Mobile computing platforms; Size; Contrast ratio of the screen; Connectivity;

EP #	EP requirements	EP key concepts
	connectivity, memory, etc.) and the external factors related to their use (varying environment as regards level of light or noise).	Memory; External factors related to their use (varying environment as regards level of light or noise)
5.8.4	Manufacturers should set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended.	Minimum requirements; Hardware; IT networks characteristics; IT security measures; Protection against unauthorized access
5.8.5	The medical device and IVD medical device should be designed, manufactured and maintained in such a way as to provide an adequate level of cybersecurity against attempts to gain unauthorized access.	Cybersecurity; Protection against unauthorized access

Table C.4: IMDRF EP 5.10 – Labelling

EP #	EP requirements	EP key concepts
5.10.1	Medical devices and IVD medical devices should be accompanied by the information needed to distinctively identify the medical device or IVD medical device and its manufacturer. Each medical device and IVD medical device should also be accompanied by, or direct the user to, any safety and performance information relevant to the user, or any other person, as appropriate. Such information may appear on the medical device or IVD medical device itself, on the packaging or in the instructions for use, or be readily accessible through electronic means (such as a website), and should be easily understood by the intended user.	Information [Manual]; Safety; Performance; Easily understood

Table C.5: IMDRF EP 5.12 – Protection against the risks posed by medical devices and IVD medical devices intended by the manufacturer for use by lay users

EP #	EP requirements	EP key concepts
5.12.1	Medical devices and IVD medical devices for use by lay users (such as self-testing or near-patient testing intended for use by lay users) should be designed and manufactured in such a way that they perform appropriately for their intended use/purpose taking into account the skills and the means available to lay users and the influence resulting from variation that can be reasonably anticipated in the lay user's technique and environment. The information and instructions provided by the manufacturer should be easy for the lay user to understand and apply when using the medical device or IVD medical device and interpreting the results.	Lay user; Self-testing; Intended use; Usage variations (user technique, usage environment); Instructions; Easy to understand; Easy to apply

EP #	EP requirements	EP key concepts
5.12.2	Medical devices and IVD medical devices for use by lay users (such as self-testing or near-patient testing intended for use by lay users) should be designed and manufactured in such a way as to:	Lay user; Self-testing; Near-patient testing
5.12.2	a) ensure that the medical device and IVD medical device can be used safely and accurately by the intended user per instructions for use. When the risks associated with the instructions for use cannot be mitigated to appropriate levels, these risks may be mitigated through training.	Safety; Accuracy; Instructions; Risk reduction; Training
5.12.2	b) appropriately reduce the risk of error by the intended user in the handling of the medical device or IVD medical device and, if applicable, in the interpretation of the results.	Risk reduction; Risk of error; Handling; Interpretation of results
5.12.3	Medical devices and IVD medical devices for use by lay users (such as self-testing or near-patient testing intended for use by lay users) should, where appropriate, include means by which the lay user:	Lay users; Self-testing; Near-patient testing
5.12.3	a) can verify that, at the time of use, the medical device or IVD medical device will perform as intended by the manufacturer, and	Verification; Intended use; Performance
5.12.3	b) is warned if the medical device or IVD medical device has failed to operate as intended or to provide a valid result.	Warning; Failure; Valid result

Table C.6: IMDRF EP7.2 – Performance characteristics

EP #	EP requirements	EP key concepts
7.2.1	Performance Characteristics IVD medical devices should achieve the analytical and clinical performances, as stated by the manufacturer that are applicable to the intended use/purpose, taking into account the intended patient population, the intended user, and the setting of intended use. These performance characteristics should be established using suitable, validated, state of the art methods. For example:	Performance characteristics; Analytical performance; Clinical performance; Validation; State of the art
7.2.1	a) The analytical performance can include, but is not limited to, a. Traceability of calibrators and controls b. Accuracy of measurement (trueness and precision) c. Analytical sensitivity/Limit of detection d. Analytical specificity e. Measuring interval/range f. Specimen stability	Traceability of calibrators and controls; Accuracy of measurements (trueness and precision); Analytical sensitivity/Limit of detection; Analytical specificity; Measuring interval/range; Specimen stability

EP #	EP requirements	EP key concepts
7.2.1	b) The clinical performance, for example diagnostic/clinical sensitivity, diagnostic/clinical specificity, positive predictive value, negative predictive value, likelihood ratios, and expected values in normal and affected populations.	Clinical performance; Diagnostic/clinical sensitivity; Diagnostic/clinical specificity; Positive predictive value; Negative predictive value; Likelihood ratios; Expected values in normal and affected populations.
7.2.1	c) Validated control procedures to assure the user that the IVD medical device is performing as intended, and therefore the results are suitable for the intended use.	Validation; Control procedures; Intended use
7.2.2	Where the performance of an IVD medical device depends on the use of calibrators or control materials, the traceability of values assigned to such calibrators or control materials should be ensured through available reference measurement procedures or available reference materials of a higher order.	Calibrators; Control materials; Traceability of values; Reference measurement procedures; Reference materials of higher order
7.2.3	Wherever possible, values expressed numerically should be in commonly accepted, standardized units and understood by the users of the IVD medical device.	Numerical values; Standardized units; User understanding
7.2.4	The performance characteristics of the IVD medical device should be evaluated according to the intended use statement which may include the following:	Performance evaluation; Intended use
7.2.4	a) intended user, for example, lay user, laboratory professional;	Intended user
7.2.4	b) intended use environment, for example, patient home, emergency units, ambulances, healthcare centres, laboratory;	Intended use environment
7.2.4	c) relevant populations, for example, paediatric, adult, pregnant women, individuals with signs and symptoms of a specific disease, patients undergoing differential diagnosis, blood donors, etc. Populations evaluated should represent, where appropriate, ethnically, gender, and genetically diverse populations so as to be representative of the population(s) where the device is intended to be marketed. For infectious diseases, it is recommended that the populations selected have similar prevalence rates.	Relevant population; Appropriate representation; Ethnicity; Gender; Genetic diversity; Representative population; Prevalence rates

C.2   IMDRF SaMDrisk categorization framework

The IMDRF publication "Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations" characterizes the medical devices by assigning different risk levels to them based on combination of the significance of the information provided by the SaMD to the healthcare decision and the healthcare situation or condition as shown in Table C.7.

Table C.7: IMDRF SaMD risk categories

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

The four categories (I, II, III, IV) shown in Table C.7 are based on the levels of impact on the patient or public health where accurate information provided by the SaMD to treat or diagnose, drive or inform clinical management is vital to avoid death, long-term disability or other serious deterioration of health, mitigating public health.

The categories are in relative significance to each other. Category IV has the highest level of impact, Category I the lowest

The criteria for determining (a) SaMD category and (b) Levels of Autonomy are explained as follows.

C.2.1   Criteria for determining the SaMD category

The criteria for determining whether an SaMD is Category IV are:
–   SaMD that provides information to treat or diagnose a disease or conditions in a critical situation or condition is a Category IV and is considered to be of very high impact.

The criteria for determining whether an SaMD is Category III are:
–   SaMD that provides information to treat or diagnose a disease or conditions in a serious situation or condition is a Category III and is considered to be of high impact.

–   SaMD that provides information to drive clinical management of a disease or conditions in a critical situation or condition is a Category III and is considered to be of high impact.

The criteria for determining whether an SaMD is Category II are:
–   SaMD that provides information to treat or diagnose a disease or conditions in a non-serious situation or condition is a Category II and is considered to be of medium impact

–   SaMD that provides information to drive clinical management of a disease or conditions in a serious situation or condition is a Category II and is considered to be of medium impact.

–   SaMD that provides information to inform clinical management for a disease or conditions in a critical situation or condition is a Category II and is considered to be of medium impact.

The criteria for determining whether an SaMD is Category I are:
–   SaMD that provides information to drive clinical management of a disease or conditions in a non-serious situation or condition is a Category I and is considered to be of low impact.

– SaMD that provides information to inform clinical management for a disease or conditions in a serious situation or condition is a Category I and is considered to be of low impact.

– SaMD that provides information to inform clinical management for a disease or conditions in a non-serious situation or condition is a Category I and is considered to be of low impact

C.2.2 Levels of autonomy

The IMDRF SaMD Categories table was revised to accounted for various levels of autonomy as shown in the shown in Table C.8 below. Additional levels have been added to the "Treat or diagnose" category:

Table C.8: IMDRF SaMD risk categories (revised)

State of healthcare situation or condition	Significance of information provided by software to healthcare decision				
	Treat or diagnose with no possible intervention	Treat or diagnose with override	Treat or diagnose with approval	Drive clinical management	Inform clinical management
Critical	VI	V	IV	III	II
Serious	V	IV	III	II	I
Non-serious	IV	III	II	I	I

Three different levels of autonomy proposed are:
1. Approval: the software may make suggestions to the user, but either it cannot take action on its own, or it requires operator approval before taking action.

2. Override: the software can take action without approval, but the operator has the ability to over-ride (cancel) the software if need be. For example, a human driver in a self-driving car can take control.

3. No Intervention: the operator is not involved in the treatment and has no ability to override the software.

C.3   Johner regulatory guidelines for AI- for medical devices

The Johner Guideline for AI-MDs is prepared and released by the Johner Institute, Germany. The guideline is published under the Creative Commons License of type BY-NC-SA. This document is managed via the version management system git or the GitHub platform. Only the documents listed in this repository are valid. Full documentation of Johner Guidelines can be found at: https://github.com/johner-institut/ai-guideline/blob/master/Guideline-AI-Medical-Devices_EN.md.

C.3.1   Johner guidelines - objectives

The objective of Johner Guidelines is to provide medical device manufacturers and notified bodies instructions and to provide them with a concrete checklist

–   to understand what the expectations of the notified bodies are,

–   to promote step-by-step implementation of safety of medical devices, that implement artificial intelligence methods, in particular machine learning,

–   to compensate for the lack of a harmonized standard (in the interim) to the greatest extent possible.

C.3.2   Johner guidelines - scope

Johner guidelines do not set forth specific requirements for the products, but for the processes. It contains the following chapters:

1.   General requirements

2.   Requirements for product development

     a)   Intended use

     b)   Software requirement specification

     c)   Data management

     d)   Model development

     e)   Product development

     f)   Product release

3.   Requirements for phases following development

C.4   FG-AI4H data and AI solution quality assessment criteria

Data and AI solution quality assessment criteria were formulated by the ITU-T Focus Group on AI for Health's DAISAM Working Group, following the data and FGAI4H-F-032-A01: Data and AI solution assessment methods, governed by FGAI4H-F-103: Updated FG-AI4H data acceptance and handling policy.

Based on these criteria, a quality assessment questionnaire was prepared to serve as a preliminary checklist intended to guide the various AI4 Health Topic Groups in following a uniform procedure for preparing the data and AI solution technical requirements specifications and submitting them in a common reporting format.

This DAISAM quality assessment questionnaire includes a glossary that contains definitions for technical terms specific to data and AI solution quality criteria. This is provided to guide the FG-AI4 Health Topic Groups in interpreting the quality assessment checklist in a clear and concise manner and in mapping the respective technical requirement specifications.

The data and AI solution quality assessment criteria are listed in Table C.9

Table C.9: FG-AI4H data and AI solution quality assessment criteria

AI Model Development Workflow	Assessment Criteria	Description	Examples
Problem Definition	Underlying Task	Underlying Task refers to the broad taxonomy followed in organizing Machine Learning (ML) Tasks based on how the solution will be applied to solve or address the specific business problem of the respective practice domain use cases. Please refer to sections- Level-1A and Level-1B of FGAI4H-C-104 for domain use-case thematic classifications)	− Classification − Regression/Prediction − Clustering − Association rule learning − Decision Support / Virtual Assistance / Recommendation systems − Matching − Labelling − Detection − Segmentation − Sequential data models − Anomaly detection and Fraud Prevention − Compliance Monitoring / Quality Assurance − Process optimization / Automation − Other
Data Preparation	Input Data Sources, Types & Formats	− Input Data refers to the subset of the dataset that is used to train the AI model − Data Type refers to the type of the different data attributes involved − Data Format refers to the standard representation formats of the different data attributes involved	Input data sources include: − Electronic Health Records (Anonymised) − Medical Images − Vital signs signals − Lab test results − Photographs − Non-medical data-Socioeconomic, Environmental, etc) − Questionnaire responses

AI Model Development Workflow	Assessment Criteria	Description	Examples
			– Free Text (Discharge / Summary, Medical History / Notes, etc.) – Other Input Data Types include: – Real valued – Integer-valued – Categorical value – Ordinal value – Strings – Dates – Times – Complex data type – Other Standard Input Data Formats include: – DICOM PS3.0 (latest versions)- for Diagnostic Image (X-Ray, CT, MRI, PET, other pathological slides, etc) – JPEG / PNG – for Static Image – MP3 / OGG – for Audio: – MP4 / MOV- for Video – SNOMED – for clinical observations/terminology – LOINC- for laboratory observations – WHO ICD-10 for disease classifications – RxNORM for Medication Code – Other

AI Model Development Workflow	Assessment Criteria	Description	Examples
Data Preparation	Output Data Types	Output Data refers to type of data generated by the AI Model, when a particular ML algorithm is applied on the Input Data	– Binary/Class output (0 or 1) as in case of classification problems – Probability output (0-1) as in case of classification problems – Continuous valued output as in case of regression problems
Data Preparation	Target Data Types	Target Data refers to the output data in the training dataset that is defined as the reference (ground truth) for AI Model validation/testing	– Binary/Class output (0 or 1) as in case of classification problems – Probability output (0-1) as in case of classification problems – Continuous valued output as in case of regression problems
AI Model Selection	Model Type	Model Type refers to the specific machine learning algorithm and its configuration that is applied on the training dataset in order to learn the Model	Broad Classification of ML Algorithms include: – Supervised Learning based algos – Linear Regression – Logistic Regression – k-nearest neighbours – Decision Trees – Random Forest – Gradient Boosting Machines – XGBoost – Support Vector Machines (SVM) – Neural Network – other – Unsupervised Learning based algos – k means clustering – Hierarchical clustering

AI Model Development Workflow	Assessment Criteria	Description	Examples
			– Neural Network – other – Reinforcement Learning based algos – Association rule learning based algos – Apriori algorithm – Eclat algorithm – Deep learning based algos – Convolutional Neural Network (CNN) – Recurrent Neural Networks (RNNs) – Long Short-Term Memory Networks (LSTMs) – Stacked Auto-Encoders – Deep Boltzmann Machine (DBM) – Deep Belief Networks (DBN) – other
AI Model Evaluation	Evaluation Metrics	Metrics used to quantify the errors and to evaluate the performance quality of the trained model on the test dataset Selection of metrics depends on the type of the problem & the type of the model under consideration	– Model Accuracy (%) – Model Accuracy -Mean & Standard Deviation – Model Accuracy –Box Plot Summarization – Root Mean Squared Error (RMSE) – Sensitivity (True Positive Rate) – Specificity (True Negative Rate) – F1-Score (class wise performance determination) – Confusion matrix – K-fold Cross-validation – Gain and Lift Charts – Kolmogorov Smirnov Chart – Gini Coefficient

AI Model Development Workflow	Assessment Criteria	Description	Examples
			− Log Loss − Area under the ROC curve (AUC) − Concordant – Discordant Ratio − Other user defined performance measures − Other
AI Model Optimization	Optimization Objective(s)	This deals with the iterative process (feedback principle) of reconfiguring or tweaking the Model Parameters to their optimal values in order to achieve the desired level of accuracy or performance score in comparison with the baseline definition. Model performance can be systematically tracked by maintaining progressive versions of Code, Model, and Data.	Optimization techniques include: − Adding or deleting Features /Attributes of the input data − Aggregating or Decomposing Features /Attributes of the input data − Tuning Model Hyper-parameters − Normalization & Standardization of input data − Changing the learning rate of the algorithm − Examining the Statistical Significance of results − Recruiting Ensemble Methods for combining / augmenting the prediction scores of multiple models − Monitoring and tracking API response times and Computational Memory requirements of the serving infrastructure − Etc.
Safety Standards Compliance	Safety tool(s)training	This deals with the user training/orientation given on how to identify potential human safety risks occurring due to accidental or malicious misuse of the technology involved in AI Model deployment	Safety Risk Mitigation and Management Plan & Procedure
	Safety tool(s) deployment	This deals with the incorporation of necessary preventative system measures/tools as per the defined Risk Mitigation Plan to ensure that no damage or harm is caused to human safety out of	− Adopting governance procedures to assert alternative system fault tolerance plans − Adopting security mechanisms like

AI Model Development Workflow	Assessment Criteria	Description	Examples
		potential physical or cyber-attacks on the AI Model being applied.	o Authentication o Role based Access Control o Encryption o Transport Level Security o Informed Consent o Anonymisation o etc − Maintaining Data Audit Logs for secure content verification, based on o Blockchain Technology o Merkle Trees o etc − Implementing Security Standards based onDigital Certificate, SSL, SHA-256, etc
AI Model Testing	Test Data Quality Tests	Test Data refers to the subset of the dataset and not part of the training dataset that is used to evaluate the ML Model accuracy after its primary vetting by the validation dataset Quality tests are performed to minimize the noise and variance of the test data in order to maximize the performance accuracy of ML algorithm applied on it	Standard Test Options include: − Training and testing on the same dataset − Split tests − Multiple split tests − Cross validation − Multiple cross validation − Statistical significance

C.5   ITU ML5G high-level requirements mapping to AI for health requirements

Requirements analysis was performed on the ITU-T FG-ML Technical Specification "Unified architecture for machine learning in 5G and future networks" to identify high-level requirements that could be translated and applied for regulatory assessment of AI-MDs. The list of high-level requirements is given in the following tables.

ITU ML5G Req. Code	ML-unify-001
Requirement	Multiple sources of data are recommended to be used to take advantage of correlations in data.
Description	In future networks, sources of data may be heterogeneous, integrated with different NFs, and may report different formats of data. These varied "perspectives" can provide rich insights upon correlated analysis.
	Example: Analysis of data from UE, RAN, CN and AF is needed to predict potential issues related to quality of service (QoS) in end-to-end user flows.
	Thus, an architecture construct to enable the ML pipeline to collect and correlate data from these varied sources is needed.

ITU ML5G Req. Code	ML-unify-005
Requirement	Logical entities of the ML pipeline are required to be capable of splitting their functionalities or be hosted on separate technology-specific nodes. Similarly, multiple logical entities are required to be capable of being implemented on single node.
Description	In future networks, HAS for NFs will optimize the location and the performance accordingly. The network function virtualization orchestrator (NFVO) plays an important role in this. To carry forward such benefits to the ML use case, similar optimizations should also be applied to ML pipeline nodes. Moreover, the constraints applicable to an ML pipeline [e.g., training may need a graphic processor unit (GPU) and may need to be done in a sandbox domain] may be unique.
Relevance for Healthcare / Assessment	This roughly falls into the category of distributed training / inference / federated learning.
Required / Recommended?	Recommended

ITU ML5G Req. Code	ML-unify-011
Requirement	Intention is required to specify the sources of data, repositories of models, targets/sinks for policy output from models, constraints on resources / use case.
Description	The separation between technology agnostic part of the use case and technology-specific deployment (e.g., 3GPP) is captured in the design time of future network services. Intent specification for the ML use cases achieves this separation for the ML overlay. See clauses 3.2.5 and 3.2.6 for definitions.
Relevance for Healthcare / Assessment	Specification of data sources is required to provide transparency on robustness, e.g. to exclude misfit situations with unclear model outcome.
Required / Recommended?	Required

ITU ML5G Req. Code	ML-unify-017
Requirement	Model training is required to be done in the sandbox using training data. A sandbox domain is recommended to optimize the ML pipeline. Simulator functions hosted in the sandbox domain may be used to derive data for optimizations.
Description	Model training is a complicated function, it has several considerations: use of specific hardware for speed, availability of data (e.g., data lakes), parameter optimizations, avoiding bias, distribution of training (e.g., multi-agent reinforcement learning), the choice of loss function for training. The training approach used exploration of hyper parameters, for example. Moreover, in future networks, operators will want to avoid service disruptions while model training and updates are performed. These considerations point to the use of a simulator for producing the data for training the models, as well as its use in a sandbox domain.
Relevance for Healthcare / Assessment	Separation of development and production setting is required because uncontrolled, continuous learning imposes the risk of unexpected model biases.
Required / Recommended?	Required

ITU ML5G Req. Code	ML-unify-018
Requirement	The capabilities to enable a closed loop monitoring and update, based on the effects of the ML policies on the network, are required.
Description	Closed loop is needed to monitor the effect of ML on network operations. Various KPIs are measured constantly and the impact of the ML algorithm on them as well as on the ML pipeline itself (due to operations of the MLFO) are monitored and corrected constantly. These form inputs to the simulator that generate data. These data can cover new or modified scenarios accordingly in future (e.g., a new type of anomaly is detected in the network, the simulator is modified to include such data. which can also train the model to detect that data type).
Relevance for Healthcare / Assessment	Sounds like monitoring of ML algorithm performance in the production setting. Reasonable thing to do in order to be able to intervene if outcomes don't hold up to expectations and might cause risks to patient safety.
Required / Recommended?	Required

ITU ML5G Req. Code	ML-unify-019
Requirement	A logical orchestrator (MLFO: ML function orchestrator) is required to be used for monitoring and managing the ML pipeline nodes in the system. MLFO monitors the model performance, and model reselection is recommended when the performance falls below a predefined threshold.
Description	The varied levels and sources of data (core, edge), including the simulator and the sandbox domain, imply that there could be various training techniques including distributed training. Complex models that are chained (or derived) may in fact be trained using varied data. The performance of such models can be determined and compared in the sandbox domain using a simulator. Based on comparisons, operators can then select the model for specific use cases. This can be used in

ITU ML5G Req. Code	ML-unify-019
	conjunction with the MLFO to reselect the model. NOTE: evaluation may involve network performance evaluation along with model performance.
Relevance for Healthcare / Assessment	Sounds like previous point, monitoring of model outcomes

C.6   DIN SPEC 92001 - AI devices life cycle processes requirements

DIN SPEC 92001-1, Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 1: Quality Meta Model; ICS 35.080; 35.240.01

C.6.1   Introduction

Challenge: For these reasons, quality assessment of an AI module still poses a major challenge. It becomes more difficult to confirm, verify, and validate an AI module during conception, development, deployment, operation, and retirement which are wide-ranging tasks.

Abstract: This document introduces an AI quality meta model to outline key aspects of AI quality including the previously mentioned AI quality pillars. For AI quality analysis, an approach for risk evaluation and a suitable software life cycle are provided. The given AI life cycle is consistent with the international standard for systems and software engineering. The second part of this specification, DIN SPEC 92001-2, provides specific AI quality requirements.

Scope	
Purpose	Establish a quality-assuring and transparent life cycle of AI modules. Critical quality criteria are identified, and AI-specific problems are addressed. To achieve this, this document presents a set of quality requirements that are structured in an AI specific quality metamodel. It is important to note that not all AI modules impose the same quality requirements. document proposes the differentiation between AI modules with regard to their safety, secure
	The document outlines and defines the three central quality pillars functionality & performance, robustness, and comprehensibility.
Field of Application	This document applies to all life cycle stages of an AI module – concept, development, deployment, operation, and retirement – and addresses a variety of different life cycle processes.

C.6.2   Terms and definitions

For the purposes of this document, the following terms and definitions apply.

DIN and DKE maintain terminological databases for use in standardization at the following addresses:

– DIN-terminology portal: available at https://www.din.de/g

C.6.3   Quality meta model

The key quality characteristics, the so-called quality pillars, that need to be taken into account throughout the whole life cycle of an AI module, are functionality & performance, robustness and comprehensibility. These three quality pillars are not fully disjoint. For instance, robustness may be conceived as part of functionality & performance, since the adaptation to unknown environments can be a functionality requirement in a given application. In this way, AI modules are divided into two risk classes. In the following, AI modules with safety, security, privacy, or ethical relevance are summarized in components with (potentially) high risk and the latter in components with low risk. For high risk AI modules, a deviation from the quality requirements is either not permitted or is to be justified, while for low risk AI modules this is less strict.

This document, each AI module is considered to be either of high or low risk or it is assumed that a mapping of internal risk classes to high risk and low risk, respectively, is carried out. For safety, security, privacy, or ethically relevant AI modules this document requires the consideration of all listed quality requirements. Potential deviations of such AI modules need a profound justification.

C.6.3.1 AI parts module of the and AI software quality metamodel system are relation

Software systems are composed of interacting system elements, where each has its own purpose and requirements, respectively. The AI module is one of these elements that consist of AI methods and algorithms, respectively. As an element of the software system, it relates to and interacts with other elements such as hardware, software or data and with the surrounding environment such as humans. Henceforth, this document focuses on the quality assurance of AI artifacts within the software system. These artifacts can be hybrid systems. It is required to keep in mind that further standards, requirements, and regulations can apply to the overall software system and consequently to the AI module. In order to give a framework for DevOps of trustworthy AI modules, a quality metamodel is proposed and described in this document.

C.6.3.2 Risk evaluation

Risk-grade	Description
High risk	AI modules (so called "critical" AI modules) have safety, security, privacy, or ethical relevance. Domains with such relevance can be autonomous driving, medical diagnostics, and credit ratings.
Low risk	For low risk AI modules, deviations from recommended requirements are permitted without further justification. A deviation from highly recommended requirements for low risk AI modules is only permitted in exceptional cases and with appropriate justification, whereas deviations from mandatory requirements such as the establishment of a risk identification and assessment process are not accepted. Deviations from recommended and highly recommended requirements are only permitted in exceptional cases and with appropriate justification, whereas deviations from mandatory requirements are not allowed. Low risk is called "comfort" AI modules.

C.6.3.3 Environment, platform, this is our data, model

Model type	Description
Model Space	The model space includes all sets of potential approaches to solve the problem task at hand. Algorithms, mathematical models, architectures, and parameter configurations that can lead to suitable solutions for the prescribed task are included within this set.
Inference Model	The inference model is one specific element of the model space. Thus, it is composed of particular model architecture with a fixed parameter configuration. This configuration is derived from the model space via a selection method, such as a training algorithm on some data set. The inference model can be used to solve the intended task to a certain degree.

C.6.4   Life cycle

C.6.4.1 General

Stage	Definition	Context of AI
Concept	Creation of all process and defining of the problem definition, analysis, and finding a suitable model space. Based on the specific problem suitable models should be identified and analysed concerning properties like convergence and input assumptions. In this stage, no model hyper parameters are chosen and no final model evaluation is done.	Additionally, acceptance criteria should be defined for further quality assurance steps. It is, for instance, recommended to operationalize the problem such that its formulation contains possible actions for a solution.

Stage	Definition	Context of AI
Development	Means a number of activities, including the system design and specification, prototyping and implementation, integration, bug tracking and bug fixing, verification and validation including testing on various levels (functional, integration, testing, performance & robustness), packaging, documentation, versioning, etc.	Data driven development approaches are used to construct an interference model in connection with classical software engineering approaches: Such activities contain data acquisition, data analysis, and the actual programming or training efforts. In the case of ML models, the data set should be analysed, understood, and variables that are relevant for the goal or problem should be identified. In this stage, model hyper parameters are compared concerning the quality of the specific model. Different measures and metrics for the evaluation of the model quality can be considered. The aim is to find one model with specific hyper parameters that adequately solves the problem. The representation of the data set is possibly adapted to the chosen model since some ML models need a specific input shape.
Deployment	Transition from development to operation.	2 levels: a) High degree of database learning, deployment includes the training of the model on the host system and the export to the target system. b) Low degree of data-based learning: the transition from host to target system is also relevant. For instance, the acceptance of the AI module by the stakeholder is part of the target system and has to be obtained. Note that deployment starts the operation stage. Therefore, it is impossible to delineate clearly between deployment and operation.
Operation	Maintenance and evaluation aspects in the environment where the AI module is used.	Since ML algorithms can continue to learn from data through online learning and thus continue to change after training in the experimental environment.
Retirement	Disintegration and discontinuation of the AI module as well as the transition to a new AI module	This stage can be deleted from the software system or significantly changed such that a new AI module is created. This starts a new life cycle. Thus, this can be interpreted as a retirement of the original AI module as well.

One important in these stages is that everything is part of development stage.

C.6.4.2 Life cycle processes

Processes are defined by title, purpose, and outcome.

a)   Organizational project-enabling processes: This part is important to concept and provides each asset to make the project work and obtain all the expectations of company stakeholders.

Most processes within this group are only slightly affected by new challenges introduced by AI. Nevertheless, the user of this document needs to evaluate whether changes to existing processes are required. For instance, ways in which these processes need to be refined include establishing quality evaluation criteria that are applicable to functionality & performance, robustness, and comprehensibility of AI modules.

b) Technical management processes: "are concerned with managing the resources and assets allocated by organization management and with applying them to fulfil the agreements into which the organization or organizations enter [...]. In particular they relate to planning in terms of cost, timescales and achievements, to the checking of actions to help ensure that they comply with plans and performance criteria and to the identification and selection of corrective actions [...]". Additionally, specific measures with respective quality criteria need to be defined that allow evaluating if the AI module satisfies functionality & performance, robustness, and comprehensibility criteria.

c) Technical processes: "transform the needs of stakeholders into a product or service by means of technical actions throughout the life cycle". They ensure that sustainable performance and overall quality is reached when the AI module is applied. This is the group of processes that is mostly affected by AI-specific challenges. An important aspect that needs to be considered within the system analysis process is, for instance, to ensure the needed extent of interpretability of the AI module.

Agreement processes is a part of process group but IN THIS DOCUMENT, authors did not use.

Agreement processes "are organizational processes that apply outside of the span of a project's life, as well as for a project's lifespan. Agreements allow [...] to realize value and support business strategies for […] organizations." [3]. While agreement processes apply to the overall software system, they bear no reference to one software component and AI-specific challenges. Thus, this DIN SPEC does not include agreement processes.

C.6.4.3 AI quality pillars

AI quality characteristics in the form of requirements need to be considered.

The document introduces an approach to cover a sufficiently wide spectrum of AI-related software quality aspects and to emphasize the importance of AI-specific requirements. It enables the development and implementation of performance, robust, safe, and trustworthy AI modules.

Table C.10: Three key qualities

Key Quality	Definition	AI Meaning
Functionality & performance	The degree to which an AI module is capable of fulfilling its intended task under stated conditions.	Performance evaluation and model selection are further topics that are addressed in this quality pillar. It is required to precisely define the problem or goal before development and analyse it with respect to constraints and assumptions concerning environment, platform, data, and model. After problem analysis, potential solutions need to be formalized and evaluated. To find suitable solutions, adequate performance measures and metrics

Key Quality	Definition	AI Meaning
		shall be chosen for the given task and data.
Robustness	The ability of an AI module to cope with erroneous, noisy, unknown, and adversarial input data. Due to the complexity of the AI module's environment that can result from its non-stationary and high-dimensional, robustness is a key AI quality issue.	Therefore, the AI module's robustness needs to be adequately quantified and meet requirements that are defined in the risk analysis. The dependence of the model on environment, platform, and data has to be considered. Distributional shifts occur when the AI module is exposed to data points outside the training or testing data set. The possibility of an adversarial attack must be specifically addressed, since this poses a major risk to the operation of AI modules in safety and security relevant settings. For this, the adversary's knowledge of the AI module and the perturbation scope, respectively, are to be assessed and defence strategies are required to be chosen accordingly and continuously monitored during development and deployment.
Comprehensibility	The degree to which a stakeholder with defined needs can understand the causes of an AI module's output. The causes include the reason for a specific output, i.e. the input leading on to it, and the whole process of decision-making.	This means that the AI component is transparent and explainable. Furthermore, a qualitative understanding between the input variables and the response is provided with respect to the stakeholder's level of expertise and need for comprehension. For instance, the developer of an AI module needs to understand not only the data and inference model but also the model space and the mathematical framework. This quality pillar focuses on the transparency and interpretability of the chosen model. If you do not explain to the stakeholder clearly (white-box), you can create some difficulties to the project (grey-box or black-box).

C.6.5   Conclusion of quality assurance

Three parts of quality assurance is the life cycle, influencing factors, and three quality pillars. The project manager needs to join different points like the influencing factors environment, platform, data, and model. It raises awareness of possible quality issues that can arise during the different life cycle stages and processes of the AI module. The points to consider when the project manager in the life cycle is guided by the three qualities. All requirements for quality assurance are collected in these quality characteristics. Thus, the AI quality meta model covers all aspects of AI quality assurance.

C.6.6   Bibliography

Systems and software engineering– Software life cycle processes. ISO/IEC/IEEE 12207:2017.https://www.iso.org/standard/63712.html

C.7   IT Security Guidelines

C.7.1   Meta information

C.7.1.1 Guideline objectives

The objective of these guidelines is to provide medical device manufacturers and notified bodies with instructions and a specific checklist in order to:
–   Explain what notified bodies' expectations are

–   Encourage the step-by-step implementation of IT security for medical devices

–   Compensate for the absence of a harmonized standard (until there is one) as well as possible

Unlike a lot of other guidelines on IT security, these guidelines only relate to medical devices and focus on patient safety.

These guidelines are **not** intended to act as a textbook or guidelines for implementing IT security. Instead, they are intended as a guide for reviewing IT security.

The annex details the considerations that led to the creation of these guidelines.

C.7.1.2 Scope of application

These guidelines are intended for manufacturers of medical devices, especially networkable medical devices, and their service providers, as well as for people and organizations who have to evaluate the IT security of these devices.

It focuses on the IT security of the medical devices, not the organization's IT security.

The guidelines are also suitable for assessing the technical measures required for data protection. Nevertheless, the focus is on patient safety, not the confidentiality of data.

C.7.1.3 Notes on use

C.7.1.3.1   Structure of the guidelines

These guidelines are based on the idea that IT security is based on three fundamental pillars:
1.   Process requirements

2.   Product requirements

3.   Documented evidence that these process and product requirements have been met

The structure of these guidelines is based on these ideas: In section C.7.2 it starts off with the general requirements, in section C.7.3 it establishes the process requirements (including documentation), and in sectionC.7.4 it establishes the product requirements (including documentation). Within these "main chapters", the requirements are structured along software life cycle process lines:
1.   Process requirements

  a)   Requirements for the development process

1. Intended purpose and stakeholder requirements

2. System and software requirements

3. System and software architecture

4. Implementation and development of the software

5. Evaluation of software units

6. System and software tests

7. Product release

b) Requirements for the post-development phase

8. Production, distribution, installation

9. Market surveillance

10. Incident response plan

2. Product requirements

a) Preliminary remarks and general requirements

b) System requirements

c) System and software architecture

d) Support materials

The risk management requirements are woven into the requirements throughout the product life cycle.

C.7.1.3.2   Applicable chapters and requirements

Manufacturers should first use the guidelines to check the completeness of the specification documents (procedural and work instructions, checklists, etc.). For this, they should look at sections C.7.2 to C.7.4.

Subsequently, they and the people who evaluate IT security on a product-specific basis (including internal and external auditors and technical documentation reviewers) should use the guidelines to evaluate IT security for the product. In this case, they can use sections C.7.3 and C.7.4 of these guidelines as a checklist.

These guidelines contain requirements that do not apply to all products. Manufacturers must justify the exceptions that are not obvious.

C.7.1.3.3   Prioritization

If the manufacturers are not able to meet all the requirements of these guidelines from the outset, the requirements should be met in the order of their priority (from level 0 to level 3) as far as possible and where reasonable. These levels are described in the annex.

Acceptance of the security level achieved must be evaluated.

C.7.1.3.4   Comments

These guidelines contain "comments" on most of the requirements. These comments include justifications, references, comments and, above all, tips for auditors and reviewers.

Since the German term "Sicherheit" does not distinguish exactly between the important protection aims of freedom from danger and IT security, the term security is also used to emphasize IT security. Accordingly, the term "risk" means the technical possibility of reducing freedom from danger, while the term "threat" means potential attacks on IT security.

With regard to the further development of the guidelines, there is a trend towards the implementation of the ISO 2700x series of standards. This is due to detected attempts by professional attackers, who in the future will introduce malware into medical devices via the manufacturing organization's IT infrastructure, via means of communication, configuration tools, software tools and libraries. Additional security measures will therefore have to be initiated "earlier" in the development process, which will bring IT security issues in the company to the fore.

C.7.1.3.5 Liability

These guidelines are neither a legal requirement nor a harmonized standard. Accordingly, they do not differentiate between normative and informative elements.

Instead, the guidelines bring together best practices to describe the legally mandated "state-of-the-art" as well as possible.

C.7.1.4 Authors and rights of use

These guidelines were prepared by the following authors:
–   Dr Andreas Purde (TÜV SÜD)

–   Olaf Teichert (TÜV SÜD)

–   Prof. Dr Christian Johner (Johner Institute)

Dr Georg Heidenreich (Siemens Healthcare GmbH) has made a significant contribution as a reviewer.

These guidelines are published under a BY-NC-SACreative Commons license. This requires the naming of the authors ("TÜV SÜD, Johner Institute and Dr Georg Heidenreich") and allows third parties to build on this work, e.g. to improve, but only for non-commercial purposes.

The license permits commercial use of the product for consulting purposes, including audits. However, it prohibits the commercial use of this work itself, either unchanged or amended, e.g. as brochure for sales purposes.

C.7.1.5 Document control, document identification

This document is managed via the version control system Git or the platform GitHub. Only the documents named in this repository are valid.

The version history including the respective authors can be found in the document history.

The released versions are identified as such in the repository using a tag. Versions without a tag are documents in the draft stage.

C.7.2 General requirements

C.7.2.1 Process

Manufacturers should cover all the aspects mentioned below either in the procedural instructions or in the corresponding plans in order to ensure that IT security is systematically ensured. Usually the following procedural instructions and plans are affected:
–   Development

– Risk management

– Verification and validation (if not part of development)

– Post-market surveillance and vigilance

– Service, installation, decommissioning

– Customer communication

– Management evaluation (ISO 13485 requires "applicable new or revised regulatory requirements" to be taken into account).

If the manufacturer uses outsourced processes, the requirements apply accordingly. For example, a (software) development service provider would have to observe the sections of these guidelines that are relevant for it.

C.7.2.2 Expertise

Manufacturers must ensure and demonstrate that they have sufficient expertise to ensure IT security in line with the state of the art. This evidence is often most easily obtained through internal or external training.

In this way, manufacturers can also access the expertise of external resources.

ID	Requirement	Level	Comments
	The manufacturer has created a list of all roles that are directly or indirectly involved with IT security.[1]	1	
	The manufacturer has provided evidence of the IT-security expertise for each role.[2]	1	
	The manufacturer has records (e.g. training documents) that lead to the conclusion that the people in question actually have this expertise.	1	
	The (software) development plans define the (additional or deviating) expertise on a product-specific basis.	2	Requirement since ISO 13485:2016.

C.7.2.3 Documentation

The manufacturer should be able to provide evidence that it has complied with the relevant requirements of these guidelines. There are no specific requirements for the documentation and "objective evidence".

In Europe (unlike in the USA), there is also no obligation to create a specific document on IT security. Instead, manufacturers can integrate these aspects into existing documents, such as the QM system specification documents and the technical documentation (e.g. software files, risk management files).

C.7.3 Process requirements

C.7.3.1 Product development requirements

C.7.3.1.1 Intended purpose and stakeholder requirements

ID	Requirement	Level	Comments
	The manufacturer has identified all neighbouring systems (medical devices, IT systems) that may be connected to the product.	0	
	The manufacturer has created a list of roles (people, neighbouring systems) that may interact with the product.	0	Ask for the list of roles to be shown.
	The manufacturer has identified all markets and all the regulatory requirements that are relevant in these markets.	0	Ask for the list of IT security regulatory requirements to shown.
	The manufacturer has identified the intended primary and secondary users with their IT expertise.[3]	1	
	The manufacturer has defined the intended user environment.[4]	1	
	The manufacturer has analysed the risks (hazards) that result if the system is used in the specified user environment by someone who is not a specified user.[5]	1	
	The manufacturer has described in the risk management documentation what the IT security threats are and what the consequences would be for patients, users and third parties.	1	
	The manufacturer has traceably generated the risk acceptance criteria based on the product's use and the state-of-the-art.	1	
	The manufacturer has developed a system it can use to evaluate IT security-related risks.[6]	2	

C.7.3.1.2 System and software requirements

C.7.3.1.2.1 Authentication and authorization

ID	Requirement	Level	Comments
	The manufacturer has identified all data interfaces.	0	Ask for the list of data interfaces (wired, WLAN, USB, etc.) to be shown.
	The manufacturer has specified the protocols and standards used for each data interface.[7]	1	
	For each data interface, the manufacturer has specified the functions offered via the interface.	0	Ask for the list of functions to be shown.
	The manufacturer has analysed each function's security relevance (in terms of hazards).	0	
	The manufacturer has documented the effects of the safety-relevant (in terms of hazards) functions in the risk management documentation.	0	
	The manufacturer has tested all usage scenarios[8] in which risks are generated due to a display of information that has not been specified (e.g. no display, incorrect display or display is too late).	1	Ask for this to be shown in the risk management or usability file.

ID	Requirement	Level	Comments
	For each role and neighbouring system, the manufacturer has defined the product functions that they may have access to via the corresponding interface.	1	Ask for the "mapping" of roles to functions to be shown, e.g. as a table.
	The manufacturer has justified its choice of authentication procedure (username/password, biometric procedure, token, e.g. card) for all roles and all neighbouring systems.	1	The justification should be risk-based.
	Where necessary, the manufacturer has requested additional mechanisms to minimize the probability of unauthorized access.[9]	2	
	The manufacturer has analysed, in the risk management process, the effects on patient safety if a person cannot access patient or device data (e.g. no authorization, they forget their password), and defined appropriate measures.[10]	1	This is about balancing the protection goals of "confidentiality" and "safety".

C.7.3.1.2.2   Data, communication

ID	Requirement	Level	Comments
	The manufacturer has created a list of all data managed by the system.[11]	1	
	The manufacturer has assessed how worthy of protection these data are in relation to confidentiality and their impact on patient safety.	1	
	The manufacturer has evaluated, in the context of risk management process, the effect if particularly sensitive data is no longer protected.	1	
	The manufacturer has investigated, in the context of risk management, the consequences of overloading the system with too many requests (e.g. DoS) or requests with volumes that are too large and has defined actions if necessary.	2	
	The manufacturer has, in the context of risk management, analysed the consequences of the network no longer being available or no longer being available in the expected quality.	2	
	The manufacturer has, in the context of risk management, analysed the consequences of the loss of data and establishes actions, such as making a backup, if necessary.	2	
	The manufacturer has established, in general or for specific products, the criteria[12] for the checking of external data before they are processed further.[13]	2	

C.7.3.1.2.3   Patches

ID	Requirement	Level	Comments
	The manufacturer has a documented plan of how patches are applied and removed again. This plan includes the development, distribution, installation and review of patches.	1	This plan can be part of the incident response plan (see below).
	The manufacturer has a list of all SOUP/OTS components.	1	This requirement belongs more to the "System and software architecture" section.
	The manufacturer has assessed how often patches are required and how they should be installed.	2	

C.7.3.1.2.4   Other

ID	Requirement	Level	Comments
	The manufacturer has established how the medical device informs the users in the event that cybersecurity is compromised.	2	
	The manufacturer has assessed what functionality the medical device must guarantee in the event that cybersecurity is compromised.		

C.7.3.1.3   System and software architecture

ID	Requirement	Level	Comments
	The manufacturer has documented all SOUP/OTS components (incl. version, manufacturer, reference to information on updates, release notes).	1	Ask for the list/table to be shown. The FDA requires a "Cybersecurity Bill of Materials (CBOM)".
	The manufacturer has analysed the specific risks resulting from the choice of technologies (in particular programming language, SOUP/OTS components).	2	
	The manufacturer has 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.[14]	2	
	The manufacturer has created a list of all services[15] that the product offers or uses "externally" (e.g. through its operating system).	1	Ask for this list to be shown.
	For each service, the manufacturer has justified why it has to be visible externally (no time limitation).	2	Have the manufacturer explain how/where it is required and tested that services that are not required (no time limit) are not offered (no time limit). The aim of this is "attack surface reduction".
	If the product provides an interface, the manufacturer has described how attacks via this interface are controlled in the context of risk management.	1	Complete control of these risks is generally not really possible with USB interfaces, but also not necessary in all cases.
	The manufacturer has identified the process offering/running this service for each externally visible service.	2	
	For each process, the manufacturer has identified the user (at the operating system level) and, if this user does not run with minimal rights ("worst case" as root), justified this.	2	
	The manufacturer has systematically identified the risks that would be caused by deficient IT security using threat modelling.	2	Have the model show that at least the external actors and/or threats and the threatened objects have to be identified.
	The manufacturer has analysed the risks that result from the (auto-)update of anti-malware software.	1	

ID	Requirement	Level	Comments
	The manufacturer has established how the product detects compromised IT security, document (log) this and react to it quickly.		
	With regard to the audit log, the manufacturer has determined where its data is stored, how it is protected and updated and how this can be automatically analysed.		
	For all software components[16], services and processes, and data and software components, the manufacturer has analysed which risks arise if they do not behave in accordance with the specifications due to a problem with IT security.	1	Corresponds to an FMEA approach.
	The manufacturer has taken the software requirements into account in the software architecture.	1	For example, for the above software requirements, ask for the component(s) or technologies in the architecture that implement the requirements to be shown.

C.7.3.1.4 Implementation and development of the software

ID	Requirement	Level	Comments
	The manufacturer has created coding guidelines that establish specific requirements for IT security.[17]	1	Ask the manufacturer to show the coding guidelines and corresponding requirements.
	The manufacturer only plays code where reverse engineering and RAM readout cannot lead to unacceptable risks.[18]	3	
	The manufacturer either tests the software (source code and binaries) for malicious code before delivery and/or has protected all computers involved in the development and "production" of the software against malware.	0	
	The manufacturer has defined measures that can find and eliminate buffer overflows.	2	

C.7.3.1.5 Evaluation of software units

ID	Requirement	Level	Comments
	The manufacturer has defined at least one method that is used to check compliance with the coding guidelines.	1	The manufacturer will achieve this if it uses tools for static code analysis and/or establishes specifications for the code reviews.
	The manufacturer requires code reviews for all components that map (IT) security-relevant functions.	2	
	The manufacturer has concrete test criteria[19] in its specification documents for the code reviews.	1	
	The code reviews are carried out according to the four-eye principle and only by people who have the necessary expertise. The manufacturer has documented this expertise.[20]	2	

ID	Requirement	Level	Comments
	The manufacturer has established which tests (e.g. unit tests) are necessary with which test cases[21] and which degrees of coverage are necessary.	1	
	The manufacturer has described how all SOUP and OTS components have to be verified.	1	

C.7.3.1.6 System and software tests

ID	Requirement	Level	Comments
	The manufacture includes port scans at all relevant network interfaces in the test plan[22] and also performs them.	1	
	The manufacturer includes penetration tests at all relevant data interfaces and/or for all known vulnerabilities of the OTS components used[23] in the test plan and also performs them.	2	For a known OTS component in the NIST Common / National Vulnerability Database, investigate a vulnerability and have the manufacturer explain how it ensures that it cannot be exploited or why it is not relevant.
	The manufacturer includes the use of "vulnerability scanners" in the test plan.		
	The manufacturer includes fuzz tests at all relevant data interfaces with at least one tool in the test plan and also performs them.[24]	2	
	The manufacturer includes a security check against the usual attack vectors in the test plan.[25]	2	
	The manufacturer includes the testing of robustness and performance in the test plan.		
	The manufacturer includes the testing of all system/software requirements (see above) in the test plan.	1	
	The manufacturer also has its software checked by IT security experts with regard to the above measures.	3	To reach level 3, this testing must include fuzz and penetration testing as well as analysis of the system/software architecture and the source code.
	The manufacturer includes third-party test reports (e.g. from SOUP manufacturers) in the system test (if available).		

C.7.3.1.7 Product release

ID	Requirement	Level	Comments
	The manufacturer has addressed the most common errors[26] and the resulting hazards in the risk analysis or can at least explain how these risks are controlled.	1	Select an example from one of the linked lists of the most common errors and ask the manufacturer for a justification.
	The manufacturer discusses the risks posed by all relevant attack vectors (see above) in the risk	1	

ID	Requirement	Level	Comments
	analysis and shows how these risks are controlled.		
	The manufacturer has checked the effectiveness of all risk-control measures.	1	E.g. ask for references to corresponding tests to be shown.
	The manufacturer has created a traceability matrix it uses to document that there are measures that control all risks related to IT security.	2	
	The manufacturer has prepared the risk management report and the IT security report.	2	In Europe but not in the USA, the IT security report can be part of the risk management report.
	The manufacturer has drawn up the necessary plans for the post-development phase (e.g. post-market surveillance and incident response plan).	1	Details below.
	The manufacturer has tested the completeness of the tests using a traceability matrix that links the tests to the requirements.	2	

C.7.3.2 Requirements for the post-development phases

C.7.3.2.1 Production, distribution, installation

ID	Requirement	Level	Comments
	The manufacturer has described how it ensures that only the exact intended artifacts (files) in exactly the intended version are delivered in the product or as a product.	1	This is about configuration management. Also relevant for downloads or app stores.
	The manufacturer has described how the people responsible for the installation know which is the latest version and how confusion during installation can be prevented.	2	This is only relevant for stand-alone software. A procedural or work instruction would be expected here.
	The manufacturer has described how it ensures during the installation that the requirements specified in the support materials (see above) are actually met.	1	A procedural or work instruction would be expected here.
	The manufacturer has established procedures that ensure that it can communicate quickly with operators and users of its products.	1	Level 2 is acceptable for non-critical products.

C.7.3.2.2 Market surveillance

ID	Requirement	Level	Comments
	The manufacturer has created a post-market surveillance plan.	0	
	The manufacturer has described which information is collected from the downstream phase.[27]	1	
	The manufacturer has described how and through which channels information is collected from the downstream phase.	1	
	The manufacturer has described what information is analysed and evaluated from the downstream phase.	2	Ask the manufacturer to explain how it recognizes and defines a

ID	Requirement	Level	Comments
			trend reversal and the threshold values it has set.[28]
	The manufacturer has described the resulting measures.[29]	2	Ask for the connection to the corrective and preventive actions in the process descriptions to be shown.
	For each OTS component, the manufacturer has defined at least one source through which it is informed of IT security problems and how often it is monitored[30] and described the role this analysis performs with which tools.	2	These sources should include the websites of the OTS manufacturer and the NIST Vulnerability Database.
	The manufacturer has described how it monitors that the technologies and procedures used (e.g. cryptology) are still secure.	2	

C.7.3.2.3   Incident response plan

(incl. recalls, patches, customer communication)

ID	Requirement	Level	Comments
	The manufacturer has created an incident response plan.[31]	2	
	The incident response plan governs the criteria the manufacturer uses to evaluate information from the market and when it implements the emergency plan...	2	
	Who develops and releases the patches and how and within what deadlines.	2	
	How the customer obtains the patches.	2	
	How the manufacturer ensures that the patches are also installed.	2	
	Who informs the customers, how and within what deadlines.	2	
	In which cases decommissioning or other product recalls is ordered and how.	2	

C.7.4   Product requirements

C.7.4.1 Preliminary remarks and general requirements

This section describes the product's technical functions that support IT security. They must be introduced via the requirement specification (system/software requirements) and implemented as requirements.

The following technical product measures for IT security ("security controls") must, in principle, be appropriate for ensuring the intended purpose, taking into account the intended operating environment: In order to maintain the basic requirements for safety and function, the manufacturer may waive the implementation of individual product measures in justified and documented individual cases. Therefore, for each of the following requirements, instead of implementation, the manufacturer may also include a note in the documentation (e.g. performance specifications) explaining why the requirement has not been implemented with regard to the intended purpose and taking into account the operational environment, and explaining the residual risk.

Manufacturers must check each of the measures described below to see whether they introduce new risks which themselves need to be controlled.

C.7.4.2 System/software requirements

C.7.4.2.1   Authentication

ID	Requirement	Level	Comments
	The product only allows users to use it if they have authenticated themselves to the product.	0	Ask for the associated test cases to be shown.
	The product allows the neighbouring systems (e.g. other medical devices, IT systems) connected at each data interface to exchange data only if they have been authenticated by the product.	0	Ditto The requirement that data may only be transmitted in encrypted form is set out below.
	The product allows password authentication only if this has a defined minimum length of which at least one is a non-alphanumeric character and it contains at least one uppercase and one lowercase character.	1	The choice of the authentication mechanism has been justified by the manufacturer (see above).
	The product does not have a default password or requires that a password be changed during the first use.	0	
	The product blocks users and neighbouring systems for m minutes after n attempts, with the manufacturer able to define the n and m values or their lower limits. The manufacturer has analysed the "safety-related" risks resulting from such a blocking and, if necessary, has implemented measures to minimize these risks.[32]	1	
	In the event of an unsuccessful login, the product only displays information that does not allow the user to identify the exact cause of the blocking, e.g. incorrect username or password.	2	
	The product terminates user and neighbouring system sessions after n minutes of inactivity, with the manufacturer setting the value for n or its upper limit.	2	
	The product assigns a role to each user and each neighbouring system for authentication.	1	Ask for an explanation of which software component(s)/components this functionality will be implemented in and how this is tested. The FDA even requires a hierarchical role strategy
	The product allows each role to access only the functions it is authorized for. This applies in particular for product updates/upgrades.	1	Ditto.
	The product allows authorized users to block other users and neighbouring systems.	1	
	The product allows authorized users to reset the authentication of any required elements (passwords, cryptographic keys, certificates) of other users and neighbouring systems.	1	
	The product allows authorized users to delete other users and neighbouring systems.	1	

ID	Requirement	Level	Comments
	The product does not allow users to change their own permissions.	2	
	The product allows permissions to be cancelled ("breaking the glass") and identifies/documents the person and the reasons.	2	
	In a client-server architecture, all cybersecurity measures are determined and checked on the server side.	2	
	In a client-server architecture, all client inputs are checked on the server side.	2	

C.7.4.2.2 Communication and storage

ID	Requirement	Level	Comments
	The product allows users to permanently delete all patient-specific data. The product allows you to restrict permissions to do this (e.g. to roles).	2	
	The product protects data from accidental deletion.	2	Manufacturers must check that there is no higher value security objective that prevents this, e.g. the above requirement.
	The product only transmits data (or at least security-related data) via its data interfaces in encrypted form. This also applies to storage on external data carrier.	1	Ask which encryption is used and how the initial key exchange is done.
	The product protects the integrity of the data against unwanted modification, e.g. through cryptographic procedures.	2	This applies in particular to security-relevant data, such as those mentioned in
	By default, the product rejects all incoming connections (e.g. USB, TCP, Bluetooth).	1	FDA requirement.
	The product checks all user inputs and all incoming data on the basis of verification criteria defined by the manufacturer (see above) before further processing.	1	Select an example of a data input at the user interface and the data interface and ask for the check to be shown in the code.
	The product does not use wireless transmission for the transmission of time-critical data relevant to patient safety.	2	
	The product stores passwords as "salted hash" only.	2	E.g. ask about the hash procedure and, if necessary, ask for it to be shown.
	The product stores characteristics that could be used to identify a person in encrypted form only.	2	Ask for an explanation as to what the manufacturer defines as characteristics that could be used to identify a person and which encryption mechanism it uses.
	The product protects critical data against accidental change and loss.	2	
	Every time the program is restarted, it checks whether the mechanisms used to protect the data against loss and modification are in sync.		

ID	Requirement	Level	Comments
	The product allows users to deactivate data interfaces (e.g. USB, remote access).	2	
	The product checks the integrity of the program code every time it is restarted.	2	
	In the event of that security is compromised, the product provides an emergency mode for functions that have an effect on patient safety.	2	

C.7.4.2.3 Patches

ID	Requirement	Level	Comments
	The product allows patches (own code, SOUP/OTS components) to be applied.	1	Manufacturers should be able to justify exceptions and to explain whether patching may or must be done remotely.
	The product allows you to remove defective patches again ("roll-back").	2	
	The product limits the ability to apply or remove patches to users with the corresponding permissions (authenticated and authorized).	2	
	The product checks changed program code (patches) for integrity before first use and when restarted.[33]	2	These checks are usually carried out using signatures, which themselves must be protected against forgery.

C.7.4.2.4 Other

ID	Requirement	Level	Comments
	The product logs all essential actions[34] on/in the system in an audit log, including day and time and actor (user, system).	2	
	The product ensures that it has the correct system time.	3	Have the mechanism explained. And how it is ensured that the user cannot unintentionally changed the time without noticing.
	The product protects the audit log against change.	2	Have the manufacturer explain how the protection is ensured and how a change to the audit log is identified by the system. If necessary, even ask for the responsible software components to be shown.
	The product implements mechanisms that can detect penetration or an attack[35] and react to them.[36]	3	
	The product allows the exchange of certificates.	2	

C.7.4.3 System/software architecture

ID	Requirement	Level	Comments
	The software only uses tried and tested libraries/components (no self-	1	The library must be included in the list of SOUP/OTS components. Ask the

ID	Requirement	Level	Comments
	implementation) for all cryptographic functions (e.g. encryption, signing).		manufacturer to explain the selection (criteria) to you.
	The software uses different technologies or keys for different functions (e.g. encryption of communication, encryption of data).	3	
	The software is protected against malware (viruses, worms etc.) as far as is technically possible.	1	Ask for an explanation of how the system is protected against malware and how this protection is maintained.
	The software is based on versions of the SOUP/OTS components that do not contain any security vulnerabilities. Exceptions are justified.	1	Pick an example from the SOUP list and research which version the manufacturer has and check which vulnerabilities have been patched in subsequent versions.

C.7.4.4 Support materials

The support materials refer primarily to the instructions for use and installation. If necessary, the manufacturers must also provide training materials.

ID	Requirement	Level	Comments
	The instructions for use establish the intended IT environment for operation.[37]	1	
	The instructions for use specify which activities[38] the operator must perform, as well as how and how often they should be performed.	1	
	The installation and service instructions establish which other roles (operator, service technician) are responsible for which activities[39] and how often they have to be performed.	1	
	The support materials describe how to deal with lost or stolen authentication elements (e.g. cards, certificates, cryptographic keys) and forgotten passwords.	1	
	The support materials describe how users can recognize an IT security problem with the product and what to do in this case.	2	This means that the product implements this detection.
	The support materials describe which anti-malware software has been approved for the product and where (e.g. link) it can be obtained and who is responsible for updating it.	2	Only to the extent applicable.
	The support materials contain the manufacturer's contact details, which can be used to contact the manufacturer, for example, in the event of problems with IT security.	1	
	The support materials also give a technical description of the product.	2	This is an FDA requirement in particular.

C.7.5 Prioritization

C.7.5.1 Prioritization

When prioritizing requirements, the guidelines take the following dimensions into account:
– Risk for an individual patient (combination of severity and probability of harm)

– Scope (only one patient, whole hospital, etc.)

–   Feasibility (financial and time expenditure, requirements in terms of tools)

Prioritization leads to the following maturity levels

- **Level 0 ("Layperson level")**: Even most laypeople would comply with this requirement. Anyone who does not even meet the requirements of this level should not be developing medical devices. An auditor may and must expect these requirements to be met in the very first audit.

- **Level 1 ("Advanced beginner" level)**: The manufacturer has already addressed the issue of IT security. This level can be accepted for less critical products and the initial audits. However, an improvement is expected in each subsequent year until level 2 is reached.

- **Level 2 ("State-of-the-art")**: This is the level that manufacturers generally have to reach in the long run. However, it does not yet reflect the state of scientific knowledge.

- **Level 3 ("Expert level")**: This level is reached by professional IT security experts. It goes beyond what an auditor can normally expect from medical devices. Energy suppliers, intelligence services and the military would have to operate at this level.

Depending on the risk posed by a product, an auditor or test may require a certain level from the outset[40].

C.7.5.2 Further reading

a) Laws
–   MDR

–   IVDR

–   GDPR

–   21 CFR Part 11

b) Standards and best practice guides
–   AAMI/TIR57

–   EN IEC 60601-1

–   IEC 62443-2-1

–   IEC 62443-4-1

–   IEC 62443-4-2

–   IEC 82304-1

–   IEC 80001-1

–   IEC/TR 80001-2-2

–   IEC/TR 80001-2-8

–   UL 2900-1

–   UL 2900-2-1

–   BSI-CS 132

–   ISO/IEC 29147: Information technology – Security techniques – Vulnerability disclosure

– FDA Guidance Documents

  o "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices"

  o "Post-market Management of Cybersecurity in Medical Devices"

  o "Design Considerations and Premarket Submissions - Recommendations for Interoperable Medical Devices"

  o "Wireless Medical Telemetry Risks and Recommendations"

– BSI Cyber-Sicherheitsanforderungen an netzwerkfähigeMedizinprodukte [Cyber Security Requirements for Network-Compatible Medical Devices]

c) Specialist literature, textbooks

– Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle (De Gruyter Studium)

– Johner Institute: Video trainings on the IT security of medical devices

– Current trends in Bruce Schneier's blog

C.7.5.3 Considerations

1) Manufacturers are developing more and more networked medical devices. As a result, the risks resulting from inadequate IT security (e.g. against cyberattacks) have increased. Customers are not informed about the state of the art during the procurement process and are responsible for the costs of security - before or after IT incidents. The number of IT incidents is increasing as the professionalism of attackers is rapidly increasing. Many manufacturers do not take sufficient account of this.

2) The EU regulations (MDR, IVDR) explicitly demand IT security. The EU directives demand it indirectly. These requirements can be found in the respective Annex I with the basic (safety and performance) requirements. The IT security risk analysis goes beyond the analysis of intended usage scenarios. IT security should cover scenarios outside the intended use. Therefore, the concept of foreseeable misuse must be analysed more precisely, because the manufacturer now has to take all technical possibilities of invasion into the networked medical device into account.

3) In contrast to most other basic requirements, there are no harmonized standards on IT security. Therefore, there is no canonical catalogue of requirements that is recognized as reflecting the required state of the art.

4) The FDA has published several guidance documents as well as standards such as UL 2900-2-1. These specifications are inconsistent in terms of granularity, completeness and conceptual integrity. They only meet the requirements that are usually placed on the quality of a standard to a limited extent.

5) A lot of standards are subject to charges (despite some questionable quality). In the authors' opinion, manufacturers should have free access to regulatory requirements.

6) Because most medical device manufacturers do not deal with IT security at all or only deal with it inadequately, they only meet the basic requirements. There is no consensus in Europe with regard to which technical and procedural obligations concern the manufacturer.

7)   For most manufacturers, it would not be feasible in terms of time or in terms of finance to a reach an IT security level in one fell swoop, as required by UL 2900, for example. Therefore, manufacturers should gradually strive for and reach the state-of-the-art level with regard to IT security. The aim of these guidelines is to have the initial improvements implemented quickly rather than to do nothing due to excessive demands.

8)   IT security has to be taken into account in all phases of the product life cycle process. Limiting it to testing is not enough. Together with technical product measures ("controls") and documentation, the guideline aims to refer to the three pillars of IT security: Requirements, process, documentation. The structure of these guidelines reflects these pillars and will continue to apply even after the foreseeable technological adjustments.

9)   It must be expected that standards will be developed and harmonized for medical device IT security, but this may still take years. Therefore, a guideline is needed in this intermediate phase (only).

10) These guidelines should be available soon (by November 2018) so they can provide guidance to manufacturers in the short term and allow them to act immediately. The speed of its development makes compromises in terms of cooperation with as many parties as possible unavoidable.

11) As the guidelines are based on a step-by-step convergence with the state of the art and have also been produced in a very short time, it cannot claim to be exhaustive.

12) However, the guidelines should represent an extensive and generally accepted level of requirements. The selection and priority of its requirements must therefore be as transparent as possible.

13) Such guidelines must take into account the specifics of medical devices, including the principles of patient safety and a risk-based approach. In this particular case, selected IT security measures ("controls") may conflict with the basic requirements. For this reason, there cannot be a fixed list of controls for medical devices. The medical device's intended purpose as defined by the manufacturer is vital in each case.

14) For guidelines to have the intended positive effect on IT security, it is vital that they are easy to understand and implement. Therefore, these guidelines do not set any abstract or "high level" requirements, but give binary test criteria.

15) In order to make them easier to implement, the authors also avoid bringing together as many requirements as possible. Instead, they limit themselves to the requirements they consider them to be particularly relevant and feasible.

16) These guidelines should also be and remain available free of charge in order to encourage their distribution and increase awareness of them.

17) These guidelines deliberately do not require any specific technologies or processes. On the one hand, such technologies and processes are subject to too much change, and on the other hand, the authors of the guide do not presume to decide for manufacturers which technologies and processes are best for the specific application.

18) These guidelines should be available in German and English.

19) The focus is on the IT security of medical devices, not on IT security for organizations such as hospitals and medical device manufacturers. The authors of these guidelines are aware that

attacks are increasingly affecting medical device manufacturers' supply chains. Future versions of these guidelines will have to take this into account by establishing requirements for organizations.

C.8   Cyber-security

The purpose of this appendix is to provide a brief introduction to cybersecurity. There have been many published reports, guidance, and standards relating to cybersecurity and health systems This appendix does not intend to replace those documents, but rather to provide an explanation about why cybersecurity is important and to give references for further reading. It is also important to note that cybersecurity is distinct from data privacy. This appendix does not provide information on data privacy.

Cybersecurity can be thought of as the measures taken to protect a computer system against unauthorized access or attack. Since AI solutions depend upon computer systems to function, cybersecurity is a concern for health system that utilize AI algorithms. Attackers, known as hackers, are the primary source of cybersecurity risk.

For the device developer, risk of such an attack is often difficult to quantify. Predicting the likelihood of a mechanical or electrical part failing is usually straightforward – you know how often a part is used, under what environmental conditions, the stress that it will be under--and you can design the part accordingly. However, for cybersecurity, the likelihood of something being compromised is a function of many external and qualitative criteria: How attractive of a target is your data? How secure is the network where the device is installed? How often software vulnerabilities identified and addressed? What is the cybersecurity expertise of the user?

The risk management process described in the ISO 14971:2019, "Medical devices – Application of risk management to medical devices" standard includes process steps to identify potential risks, evaluate those risks, take action to minimize those identified risks, evaluate any residual risks, and continue to monitor product performance and potential new risks.

A security management process is very similar – you identify threat sources, identify vulnerabilities, evaluate those risks, take action to minimize those risks, evaluate residual risks, and continue to monitor the product and the cybersecurity environment for potential new risks. The NIST Cybersecurity Framework is an internationally recognized document that explores these concepts in more detail.

Many regulatory jurisdictions enforce certain cybersecurity requirements or publish guidance for medical device manufacturers to consider(reference).

References:

–   AAMI TIR57:2016,Technical report Information "Principles for medical device information security risk management – Risk management",
https://store.aami.org/s/store#/store/browse/detail/a152E000006j60WQAQ

–   Pretty good list of medical cyber regulations: https://www.apraciti.com/blog/2019/11/25/global-regulatory-authority-publications-on-medical-device-cybersecurity

–   CAICT white paper on cybersecurity: https://www.dataguidance.com/news/china-caict-publishes-white-paper-cybersecurity

Annex D
AI4H project deliverables reference

Figure D.1 shows the generic as well as the AI specific aspects that need to be considered under the regulatory roadmap of medical devices. From Figure D.1, it can be inferred that AI-MD, as continuous learning or adaptive systems, are subject to modifications throughout its lifecycle and this result in unforeseen outcomes for the device including change of core device functionality and risk levels. These aspects pose additional challenges to the device manufacturers in terms of managing rapid development cycles, frequent software update and distribution cycles. Hence change management considerations tailored for AI-MDs are expected to have appropriate level of controls to manage these changes.

Figure D.2 shows the relevant AI-MD specific deliverables produced as part of the AI4H FG project. It can be seen that these AI4H deliverables include the necessary product development life-cycle processes that support the regulatory roadmap scope for AI-MDs. Document identifiers of AI4H deliverables are listed in Table-D.1- AI4H Project Deliverables Reference ID for further reference.
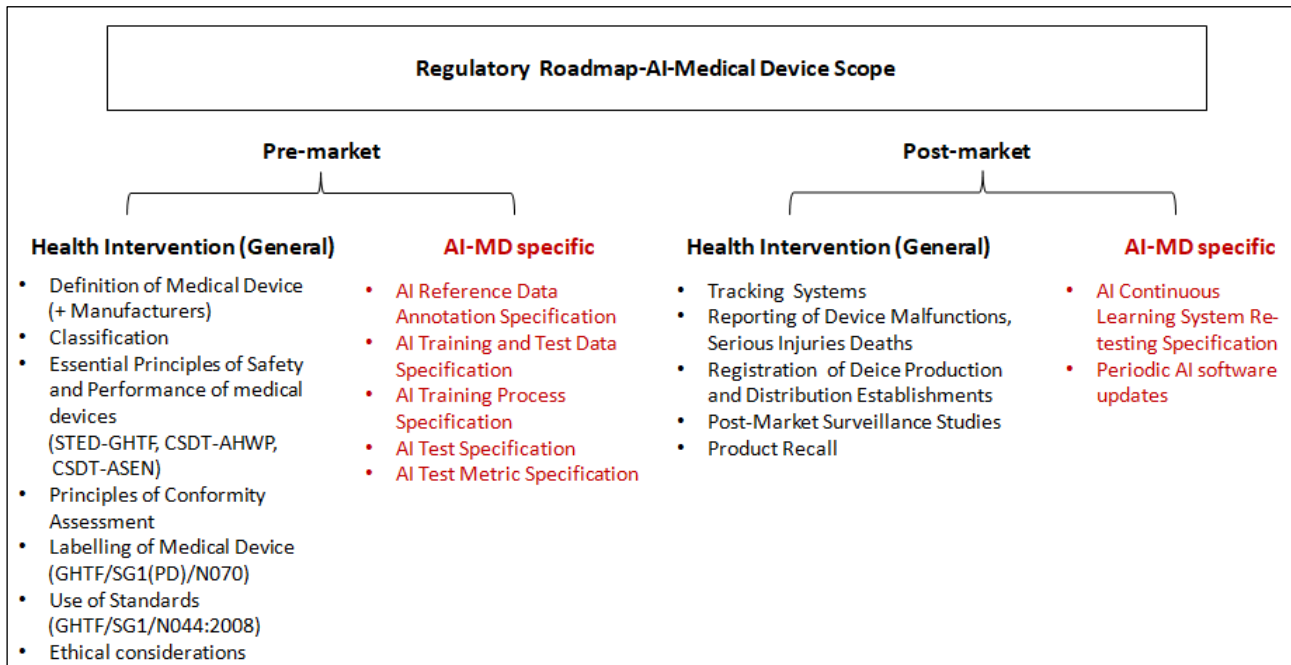

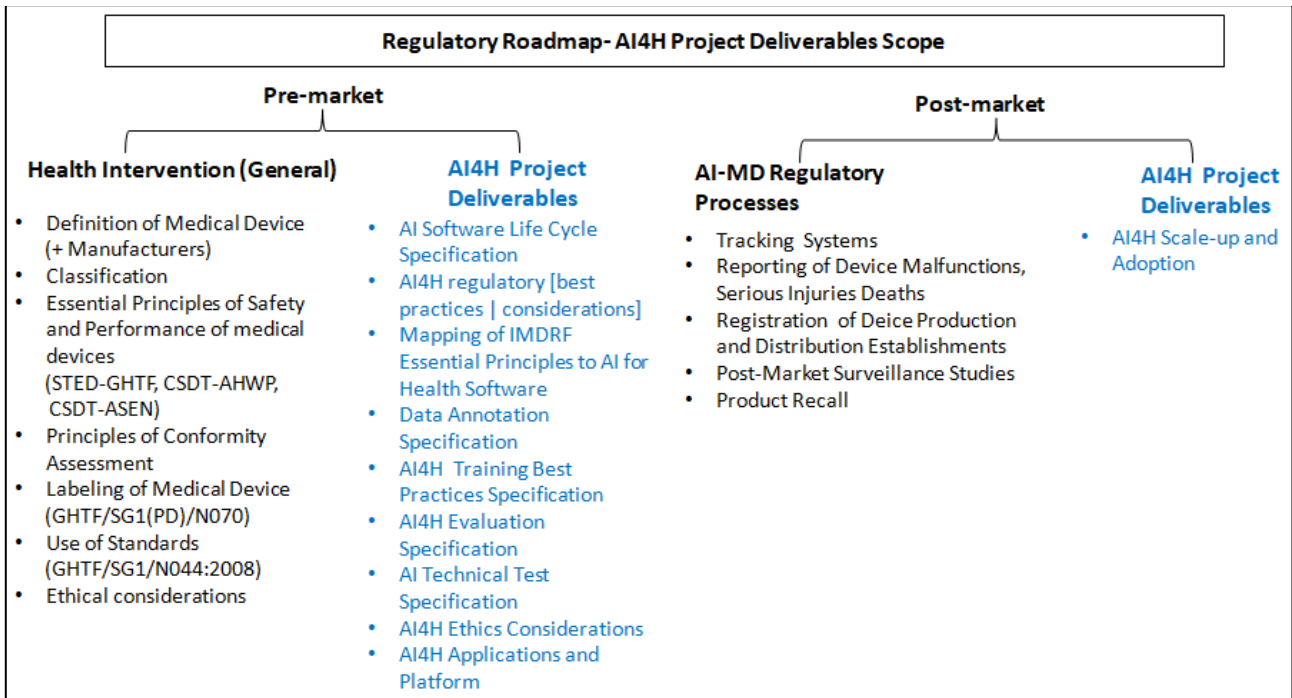**Figure D.1: Regulatory roadmap-AI-medical device scope**

Figure D.2: Regulatory roadmap- AI4H project deliverables scope

Table D.1: AI4H Project Deliverables Reference ID

AI4H Project Deliverable	ITU Document Reference ID
AI Software Life Cycle Specification	FG-AI4H DEL04
AI4H regulatory [best practices | considerations]	FG-AI4H DEL02
Mapping of IMDRF Essential Principles to AI for Health Software	FG-AI4H DEL02_1
Data Annotation Specification	FG-AI4H DEL05_3
AI4H Training Best Practices Specification	FG-AI4H DEL06
AI4H Evaluation Process Description	FG-AI4H DEL07_1
AI Technical Test Specification	FG-AI4H DEL07_2
AI4H Ethics Considerations	FG-AI4H DEL01
AI4H Applications and Platform	FG-AI4H DEL09
AI4H Scale-up and Adoption	FG-AI4H DEL08