BSI Meet the Experts Webinar

Medical Device Software and Artificial Intelligence – The BSI perspective

14 November 2023

Agenda

09:00	Welcome, agenda, BSI and Speakers Introduction	
09:05	Assessment of Medical Device Software under MDR and UKCA	Lena Gourmelon
10:30	Short break	
10:45	Artificial Intelligence in Medical Device: AI Act journey and how BSI can support Medical Device Manufacturers	Daniela Seneca
11:30	Q&A session	
11:50	Closing	

Speakers

Lena Gourmelon

Technical Team Manager, Active Medical Devices

Daniela Seneca

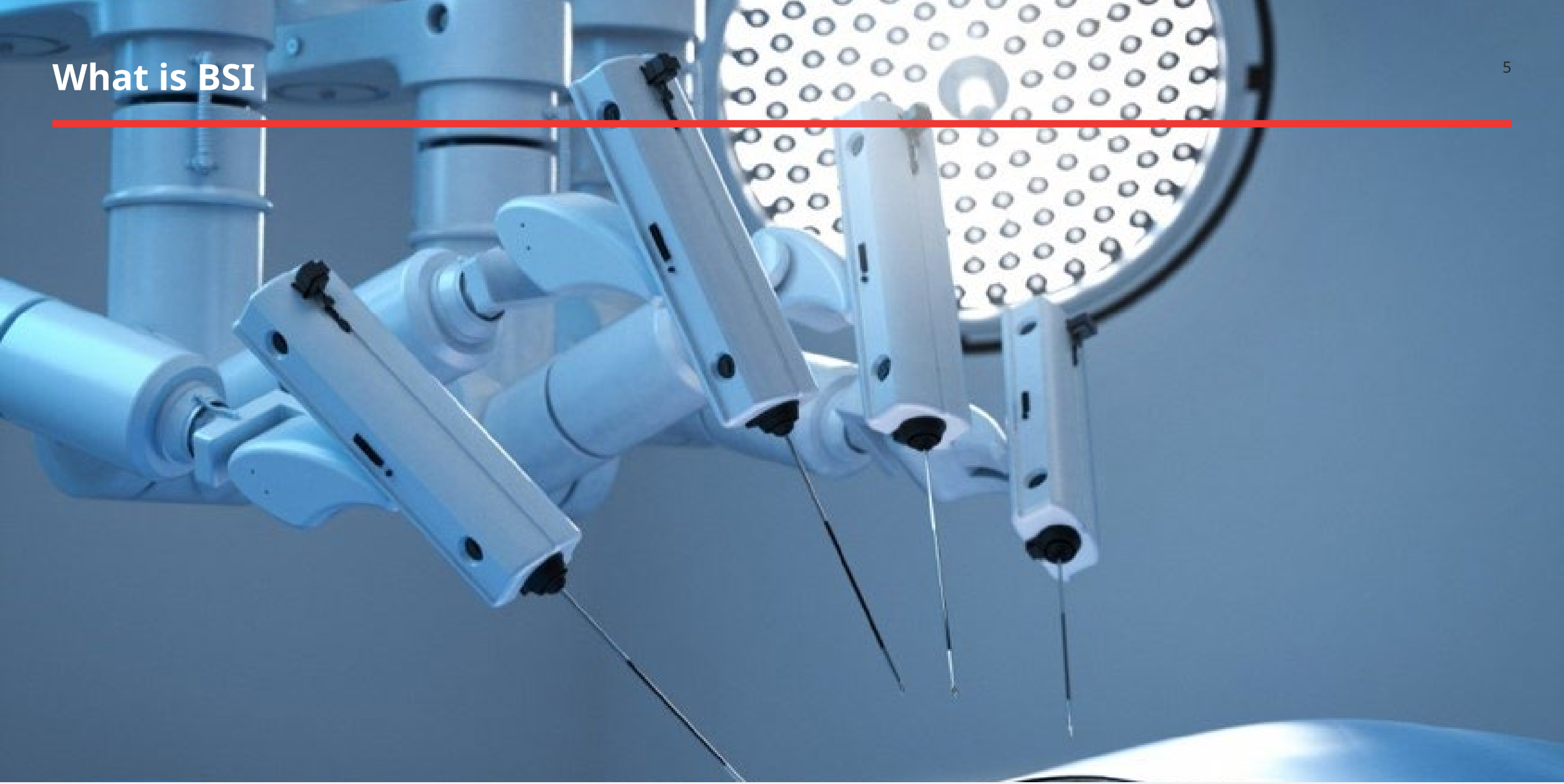
Regulatory Lead, Artificial Intelligence

Flavien Del Sole

Senior Business Development Manager

+33 6 35 81 41 24 – (Flavien.delsole@bsigroup.com)

What is BSI



BSI is…

A Notified Body for CE marking under IVDR & MDR

A Certification Body for schemes including ISO 13485, ISO 9001, ISO 14001, ISO 45001 (formerly OHSAS 18001) and ISO 27001

A recognized Conformity Assessment and Certification Body for many local market access schemes

An Auditing Organization for MDSAP

A global training provider

The UK National Standards Body

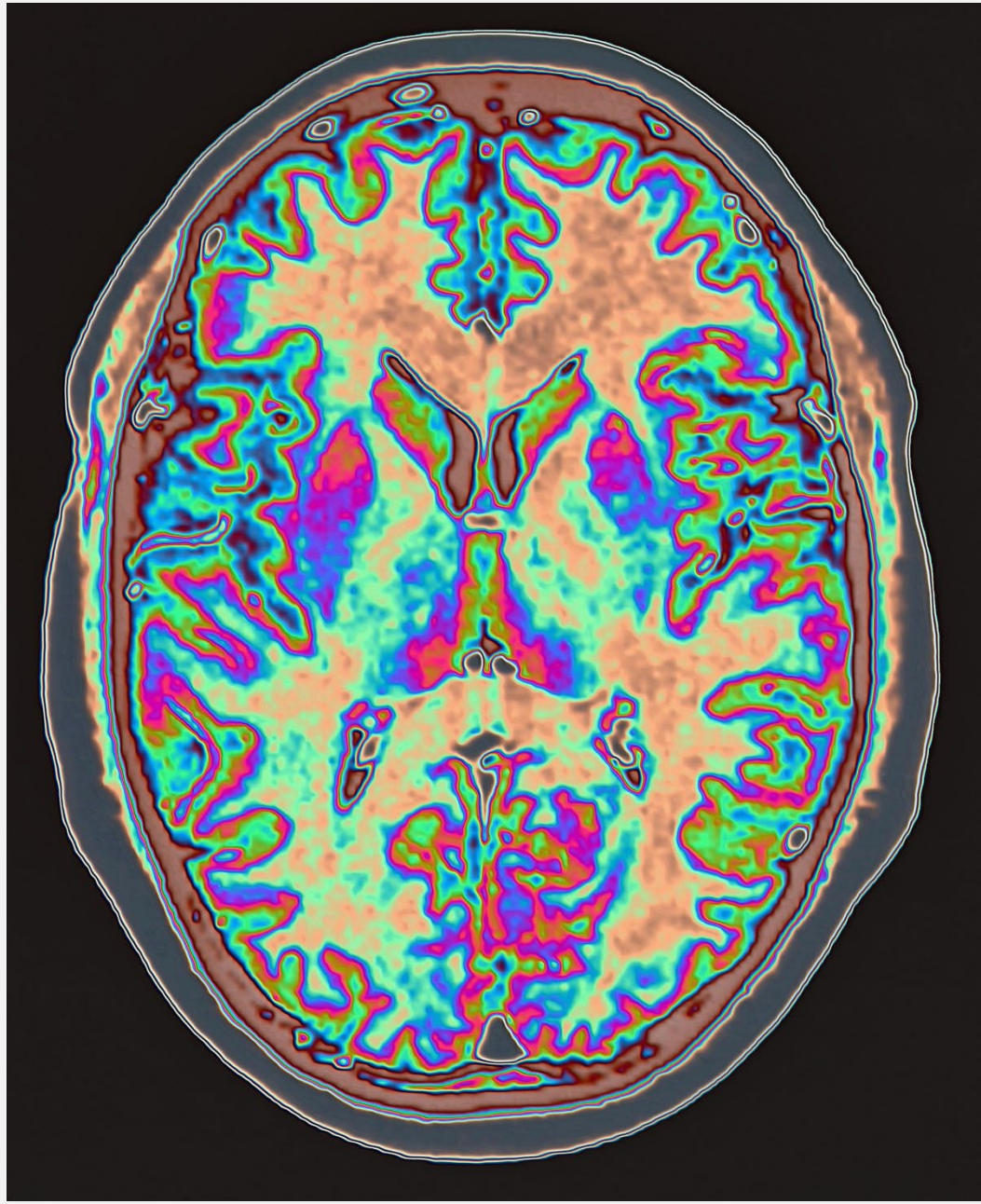
A Professional Services Portfolio
(Cyber Security Testing, Supply Chain Solutions, etc.)

bsi.

Medical Device Software (MDSW) under MDR and UKCA

Lena Gourmelon
Technical Team manager Active Medical Devices, BSI

14 November 2023



Disclaimer

What is presented today is based on our current knowledge and interpretation of the MDR and the latest available MDCG guidance

Agenda

- Intended purpose and indication for use
- Key GSPRs for software
- Important state-of-the-art standards for MDSW
- Important guidance for MDSW
- Clinical Evaluation of MDSW

Intended purpose and indication for use

The importance of defining the intended use/intended purpose

- The defined intended purpose has lot of implications. It is crucial to carefully word the intended purpose of the software medical device.
- MDR article 2 (12) - *'**intended purpose**' means the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation;*
- UK MDR 2002 - *'**intended purpose**' : the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials.*
- If the defined 'intended use'/ 'intended purpose' of the medical device software does not reflect all the claimed uses in instructions for use/promotional material/website, it is incomplete.
- An inaccurate/incomplete defined 'intended use'/ 'intended purpose' may lead to incomplete data being generated to support compliance with MDR/UK MDR 2002.

Intended purpose MHRA guidance

- The MHRA recently published a guidance on 22 March 2023: Crafting an intended purpose in the context of software as a medical device (SaMD)

  https://www.gov.uk/government/publications/crafting-an-intended-purpose-in-the-context-of-software-as-a-medical-device-samd/crafting-an-intended-purpose-in-the-context-of-software-as-a-medical-device-samd

- Although intended for use in the context of UK MDR 2002, the guidance is useful as well for defining the intended purpose under the MDR.

- Key elements of intended purpose: structure and function of the device, intended population, intended user, intended use environment.

Indication for Use

Diagnosis

Treatment

Screening

Clinical Decision support

Triage

Monitoring

Dose calculation

Definition MDCG 2020-6: *'indication', 'indication for use': refers to the clinical condition that is to be diagnosed, prevented, monitored, treated, alleviated, compensated for, replaced, modified or controlled by the medical device. It should be distinguished from 'intended purpose/intended use', which describes the effect of a device.*

Definition MHRA Guidance on intended purpose: *the clinical condition that is to be diagnosed, prevented, monitored, treated, alleviated, compensated for, replaced, modified or controlled by the medical device. It should be distinguished from 'intended purpose/intended use', which describes the effect of a device.*

Key GSPRs for Software

MDR GSPR 14

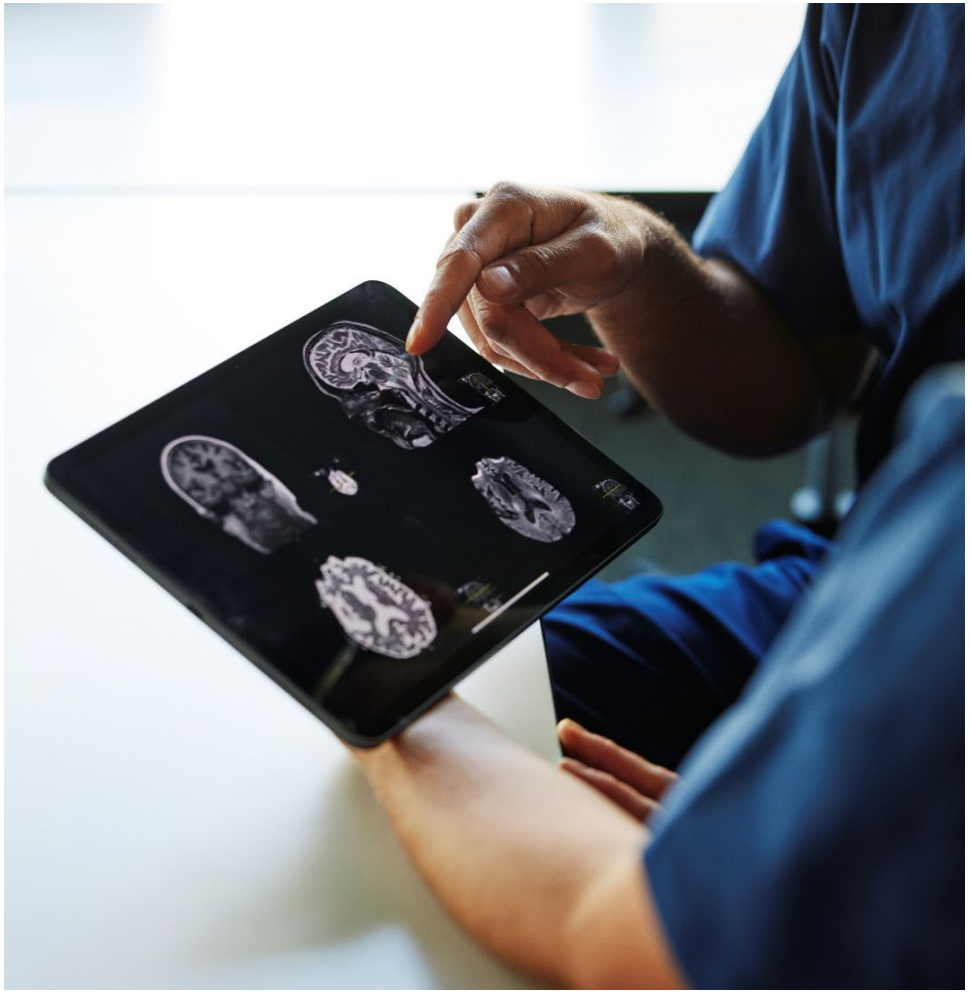
Construction of devices and interaction with their environment

MDR GSPR 14.1

If the device is intended for use in combination with other devices ***or equipment*** *the whole combination, including the connection system shall be safe and shall not impair the specified performance of the devices.* ***Any restrictions on use applying to such combinations shall be indicated on the label and/or in the instructions for use.*** *Connections which the user has to handle, such as fluid, gas transfer, electrical or mechanical coupling, shall be designed and constructed in such a way as to minimise all possible risks, such as misconnection.*

MDR GSPR 14.5

Devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the ***interoperability*** *and* ***compatibility*** *are reliable and safe.*



MDR GSPR 14

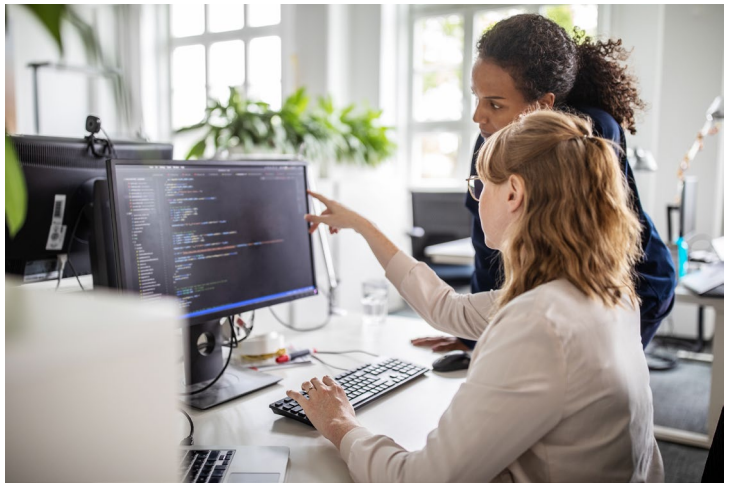
MDR GSPR 14.1 / 14.5 - Key Points

MDSW is intended for execution on non-medical equipment, e.g:

- Mobile Phones
- Tablets
- General Purpose Computers

The Notified Body will want to know:

- Are the intended platforms for the MDSW clearly defined?
- Have designated compatible MDSW/platform/OS combinations been tested to ensure interoperability to achieve expected levels of **safety and performance**?
- Are compatible platforms / restrictions on platforms specified in labelling?



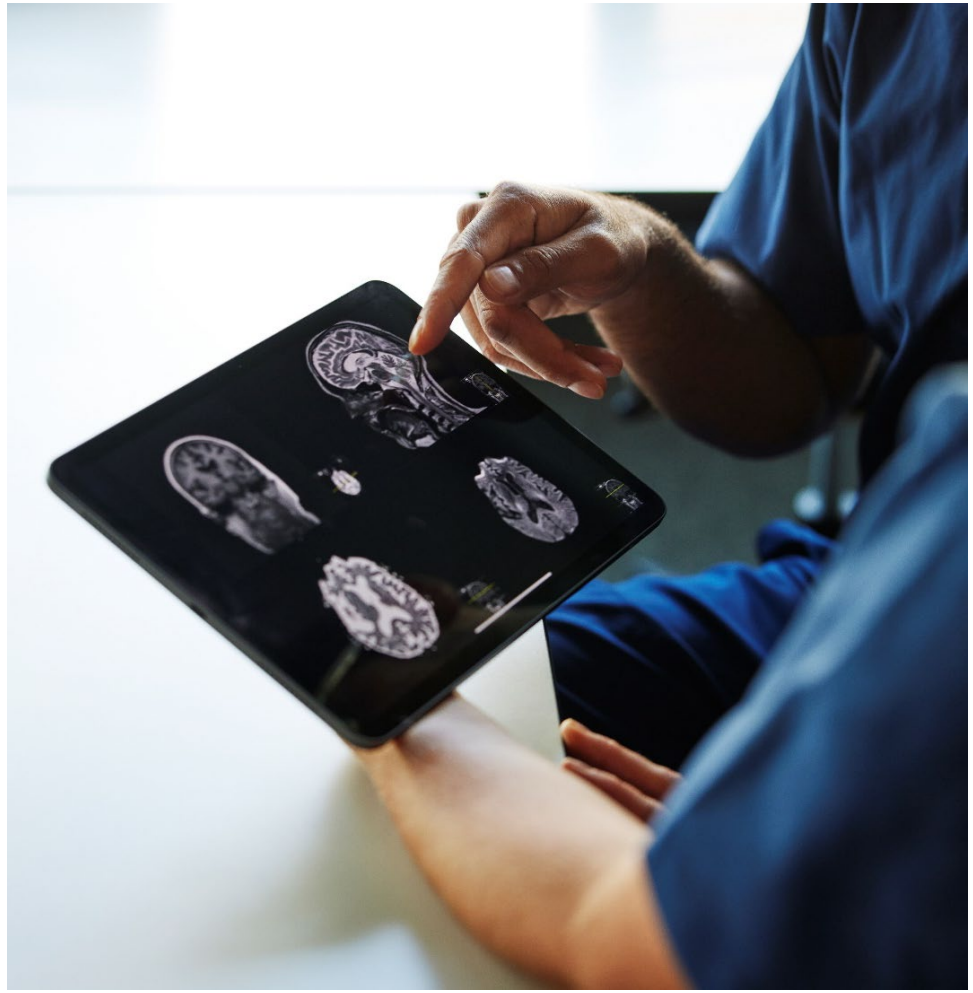
MDR GSPR 14

Construction of devices and interaction with their environment

MDR GSPR 14.2 (d)

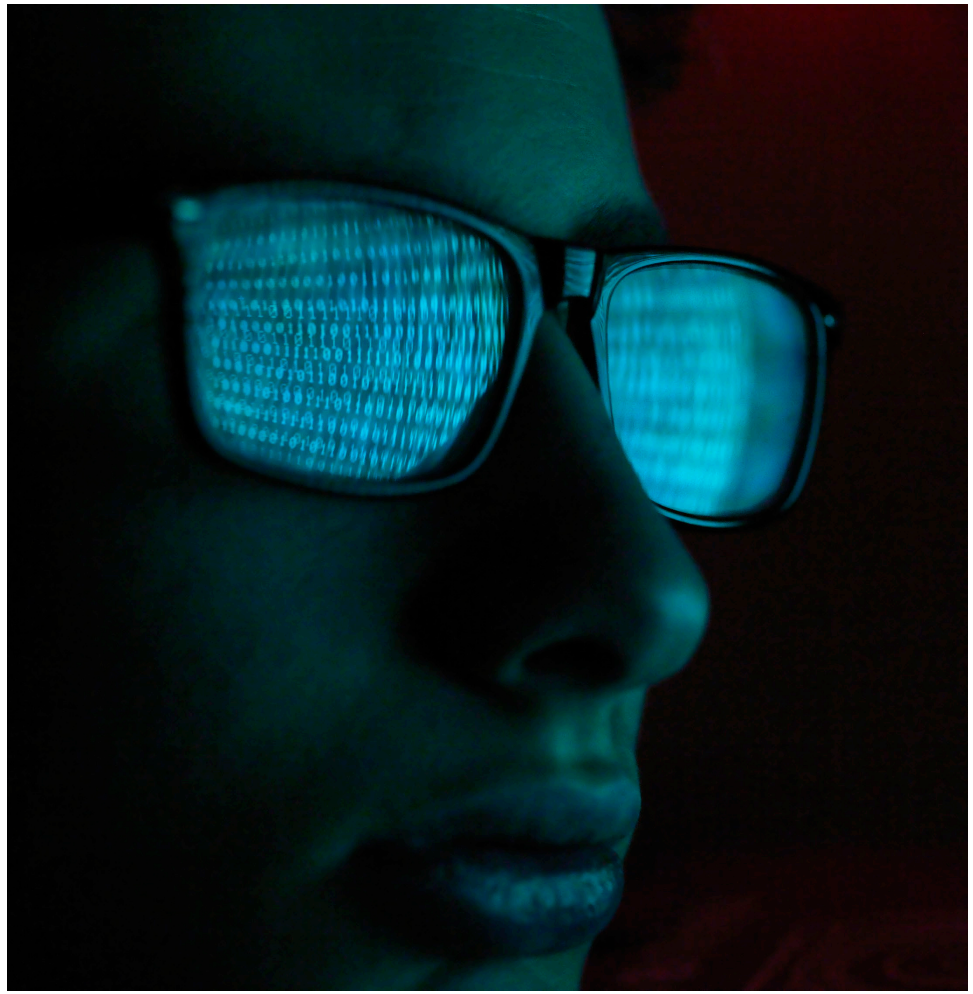
Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible: […]

(d) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;



MDR GSPR 14.2 (d) - Key Points

- What mitigations are in place to harden the MDSW against potential threats from the uncontrolled platform? E.g.:
  - Protections against alteration/removal of the MDSW from the platform?
  - How are SW/OS updates controlled/managed?
  - How are security updates/patches deployed?
- Are safety related security risks fully considered and controlled? E.g.:
  - Mitigations against threats to availability? ➔ Denial of Service Attacks
  - Mitigations against threats to integrity of data/telemetry? ➔ Man-in-the-middle Attacks
- Are risks to confidentiality considered and controlled (in addition to to risks related to safety)? E.g.:
  - Encryption of data at rest?
  - Encryption of data in transit?

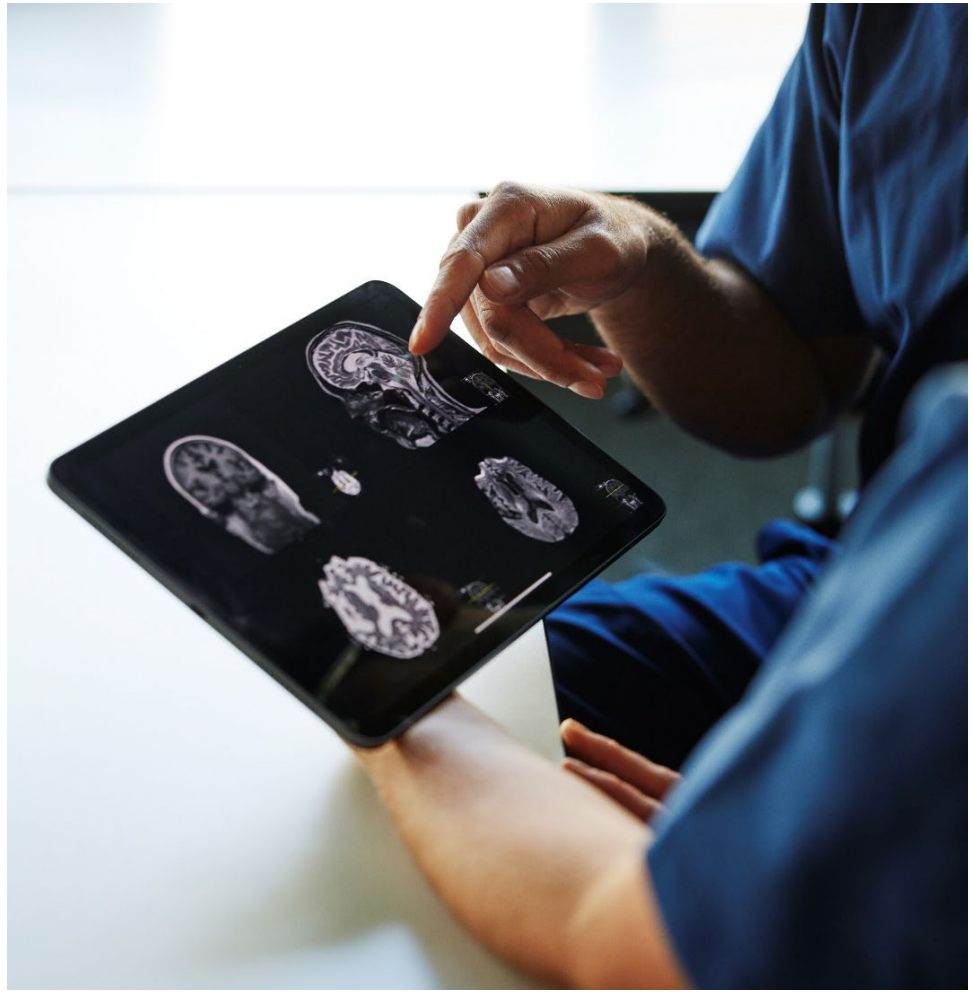


MDR GSPR 14

Construction of devices and interaction with their environment

MDR GSPR 14.7

Devices shall be designed and manufactured in such a way as to facilitate their safe disposal and the safe disposal of related waste substances by the user, patient or other person. To that end, manufacturers shall identify and test procedures and measures as a result of which their devices can be safely disposed after use. Such procedures shall be described in the instructions for use.



MDR GSPR 14.7 - Key Points

Obviously, MDSW has no physical form that requires disposal, but….

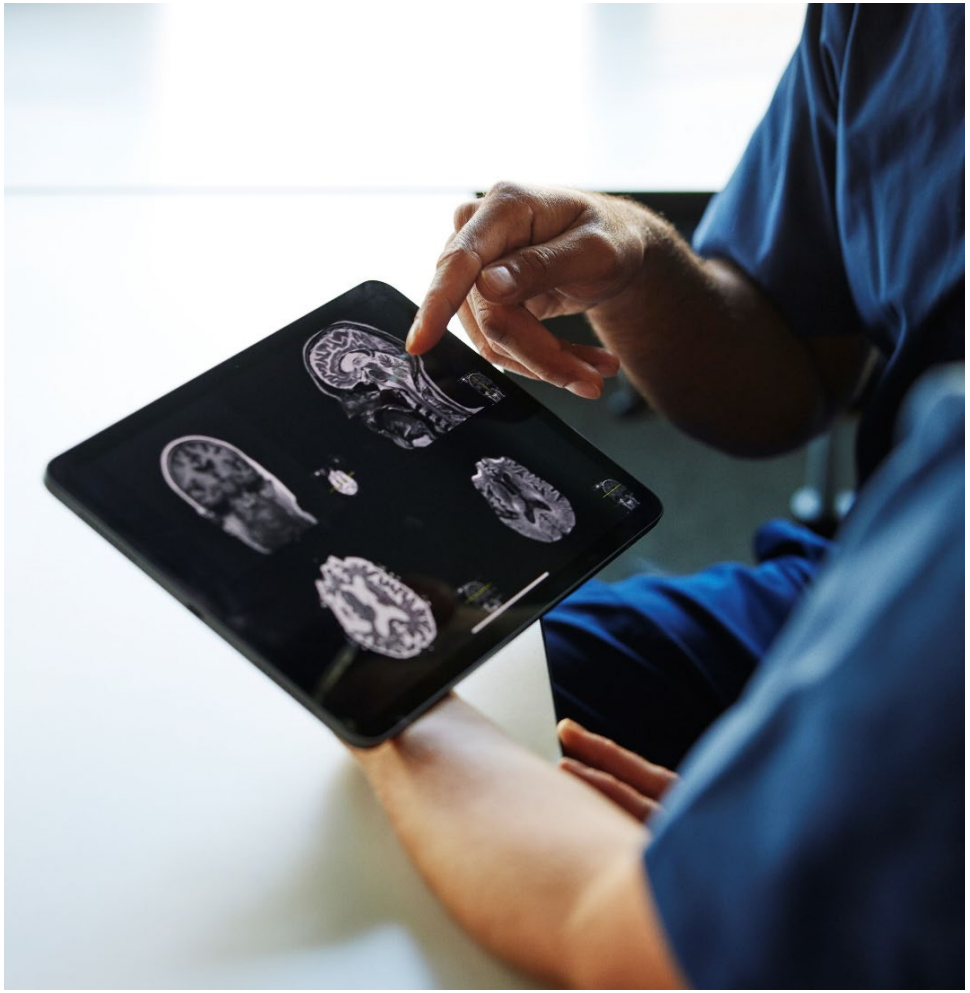
- What, if any, residual data remains on the mobile device/general purpose computer after the MDSW has been un-installed/removed?
- Does any residual data contain sensitive/confidential information (e.g. Protected Health Information)?
- Are clear instructions provided in the IFU regarding how to remove/dispose the SaMD, including any residual sensitive data

MDR GSPR 17

Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

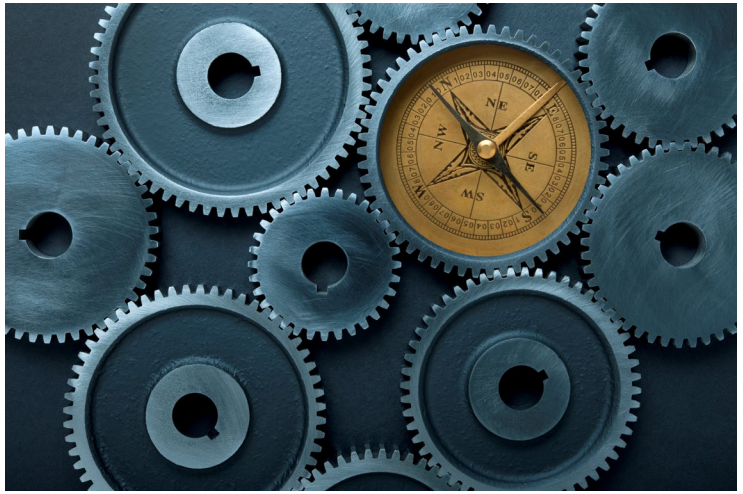
MDR GSPR 17.1

Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.



MDR GSPR 17.1 - Key Points

- Is the intended purpose of the MDSW clearly defined (e.g. diagnostic function to detect some disease state)?
- Is the intended purpose aligned across **the IFU, CER, DoC, technical documentation**?
- Are applicable requirements categories clearly defined and demonstrated via testing? (see EN 62304 Clause 5.2.2)
- Are performance requirements clearly defined in requirements and validated through testing? (e.g. Sensitivity and Specificity)
- Are risk controls implemented in software clearly established in the software requirements (or clearly traced to software requirements)?

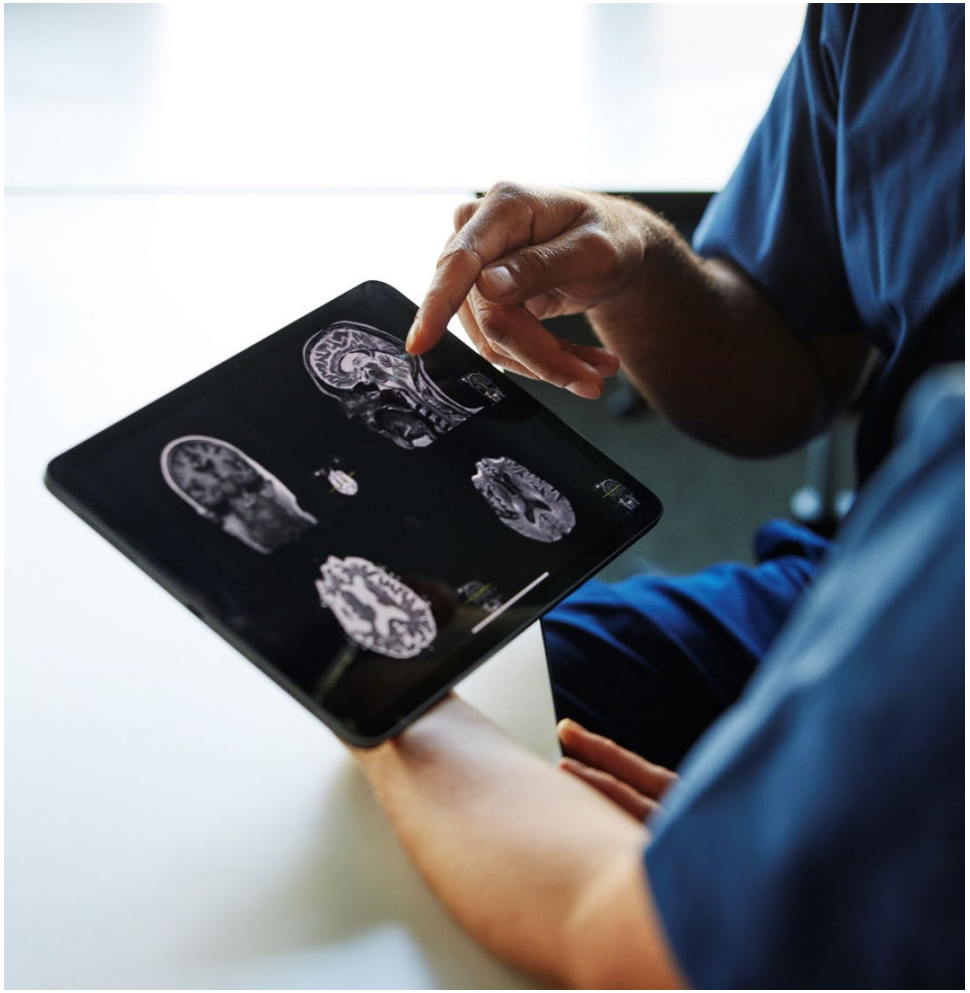


MDR GSPR 17

Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

MDR GSPR 17.2

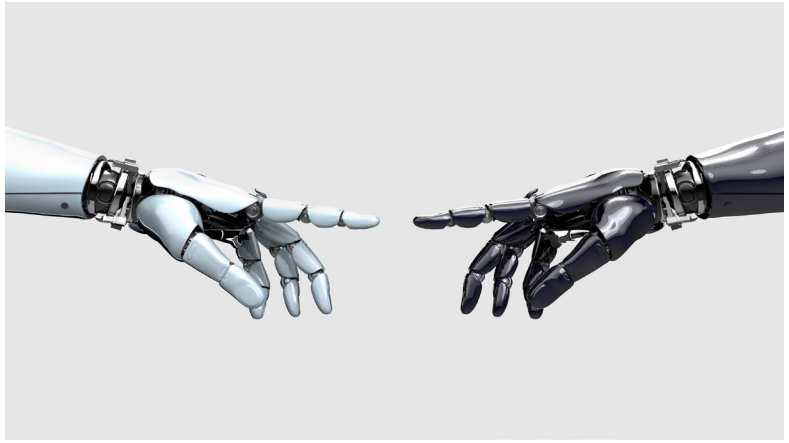
For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.



MDR GSPR 17

MDR GSPR 17.2 - Key Points

- Are development, testing, and risk management methods used representative of the state-of-the-art (SOTA)?
  - **EN 62304+A1** – SOTA for medical device software development
  - EN 82304-1 – SOTA for medical device software intended for general purpose platforms (e.g. phones, tablets, laptops)
  - EN 62366-1 – SOTA for usability engineering and usability risk management
  - **EN 14971:2019** – SOTA for risk management
- Has cybersecurity been addressed consisted with the state-of-the-art (SOTA)? Is monitoring of cybersecurity incidents and published vulnerabilities (e.g. in SOUP) part of the PMS and Vigilance process?
  - MDCG 2019-16 – SOTA for cybersecurity for medical devices
- Is clinical/performance validation and clinical/performance evaluation complete and supportive of the Intended Purpose?
  - MDCG 2020-1 – SOTA for Clinical Evaluation (MDR) of Medical Device Software

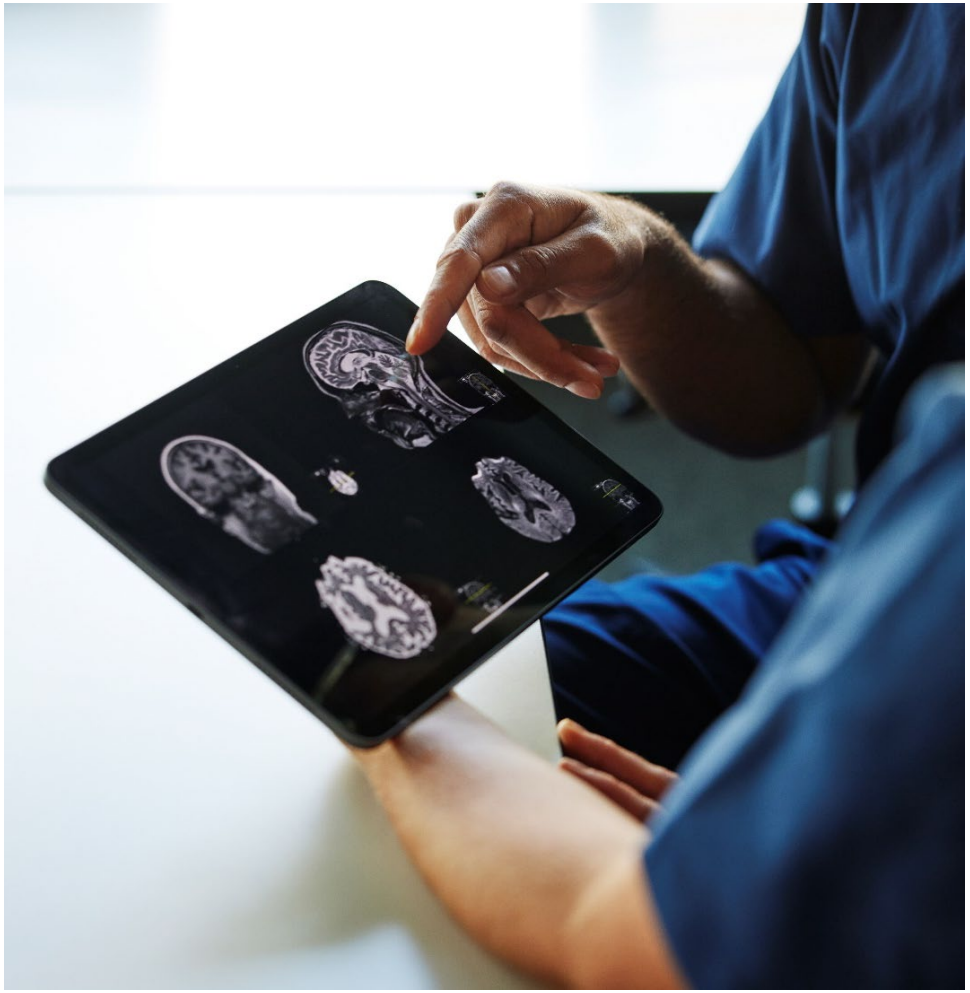


MDR GSPR 17

Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

MDR GSPR 17.3

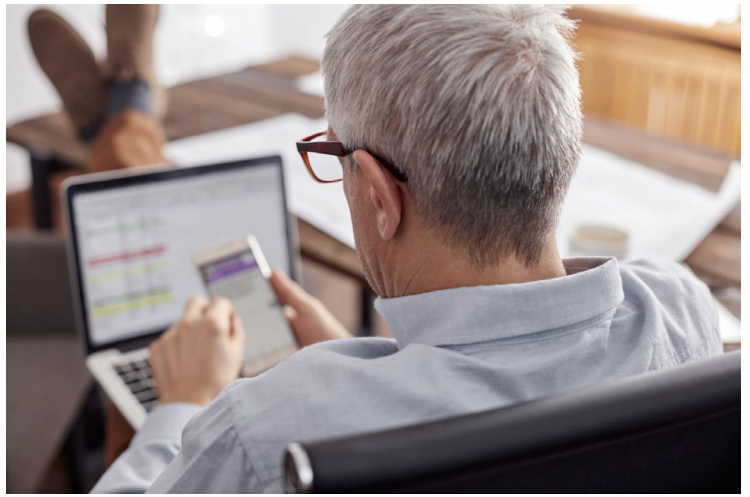
Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).



MDR GSPR 17.3 - Key Points

The Notified Body will want to know:

- Has usability testing been conducted with the intended users on the intended mobile platforms?
  - Clinical/medical professional users
  - Lay users
- Has usability testing been conducted in a simulated/actual intended use environment?
  - Clinical environment?
  - Home use environment?
  - Other possible environments?
- Have required language translation tests been conducted with multi-language software apps?
  - No truncations?
  - No overruns?
  - Error Messages clearly understandable?

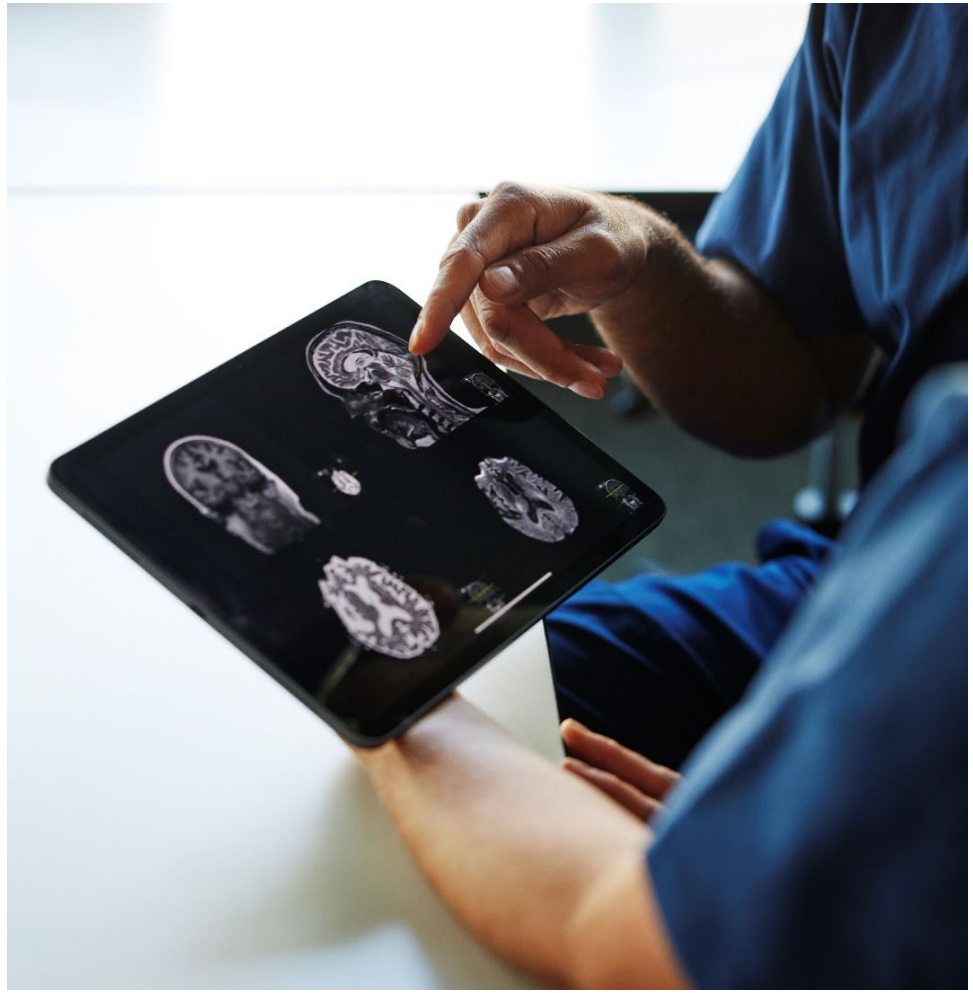


MDR GSPR 17

Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

MDR GSPR 17.4

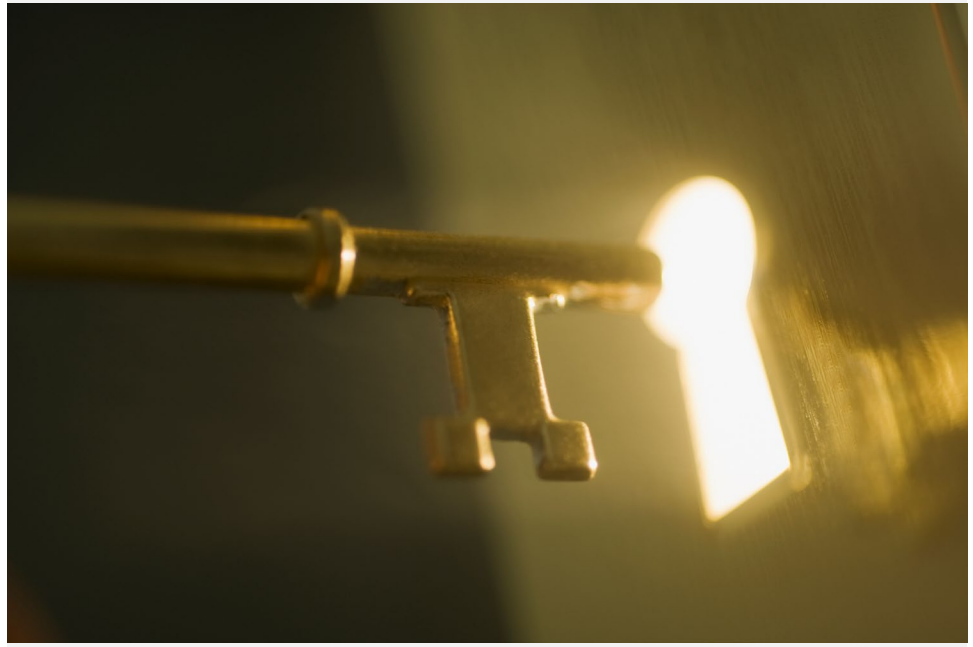
Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.



MDR GSPR 17.4 - Key Points

The Notified Body will want to know:

- Are security mitigations clearly specified in requirements documents?
- Are steps needed to configure and connect the MDSW to any external networks specified in IFUs/manuals such that expected levels of security are achieved? E.g.:
  - WiFi security set as WPA3 versus WPA2?
  - Screen locks set on “BYOD” platforms
  - Keep devices in physically secure location when not in use?
- Is user authorization implemented in the SaMD?
  - Are strong passwords enforced?
  - What mechanisms are in place to enforce password updates?



NOTE: Even if the SaMD is not designed to connect to a network or to the internet, GSPR 17.4 (MDR) still applies.

Many other GSPRs may apply for a particular MDSW based on it's **Intended Purpose**.

The GSPRs just discussed are the most common ones that generally apply to all MDSW.

Important State-of-the-Art Standards for MDSW

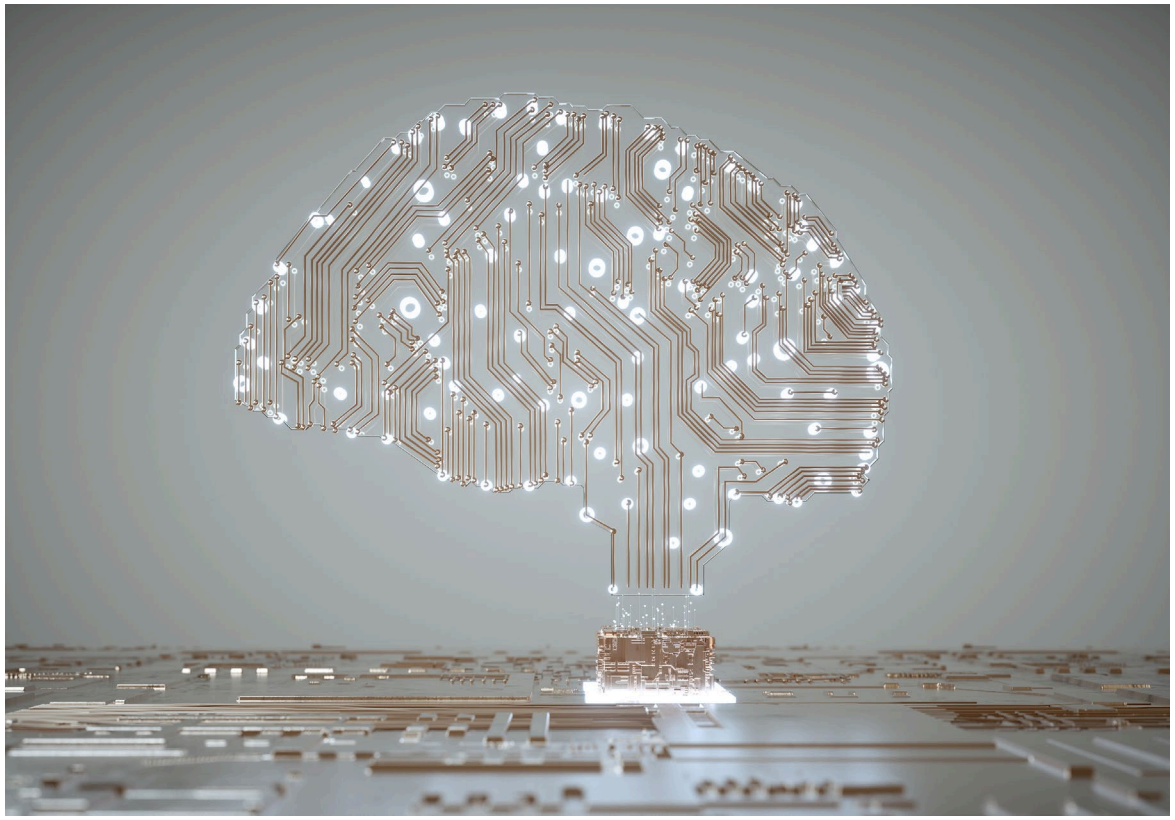
EN 62304:2006+A1:2015

Current SOTA for all MDSW

Medical device software – Software life-cycle processes

Areas covered:

- **General requirements ➔ SW safety classification** [A, B, C] ➔ Drives required activities defined in the standard
- **Software development PROCESS**
- **Software maintenance PROCESS**
- **Software RISK MANAGEMENT PROCESS**
- **Software configuration management PROCESS**
- **Software problem resolution PROCESS**



MEDICAL DEVICE SOFTWARE
SOFTWARE SYSTEM that has been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed or that is intended for use as a medical device.

EN 62304:2006+A1:2015

Key Points

- SW Safety classification adequately documented and justified based on Risk Management
- Are all required artefacts of the SW development process provided (as per SW safety class)?
  - SW Development Plan➔SW Requirements➔SW Architecture➔SW Detailed Design➔Unit Implementation & Unit Verification➔SW Integration & SW Integration Testing➔SW System Testing➔SW Release documentation
- All known anomalies documented and assessed for safety impact.
- SW risk assessment follows key principles of EN 62304

EN 82304-1:2017

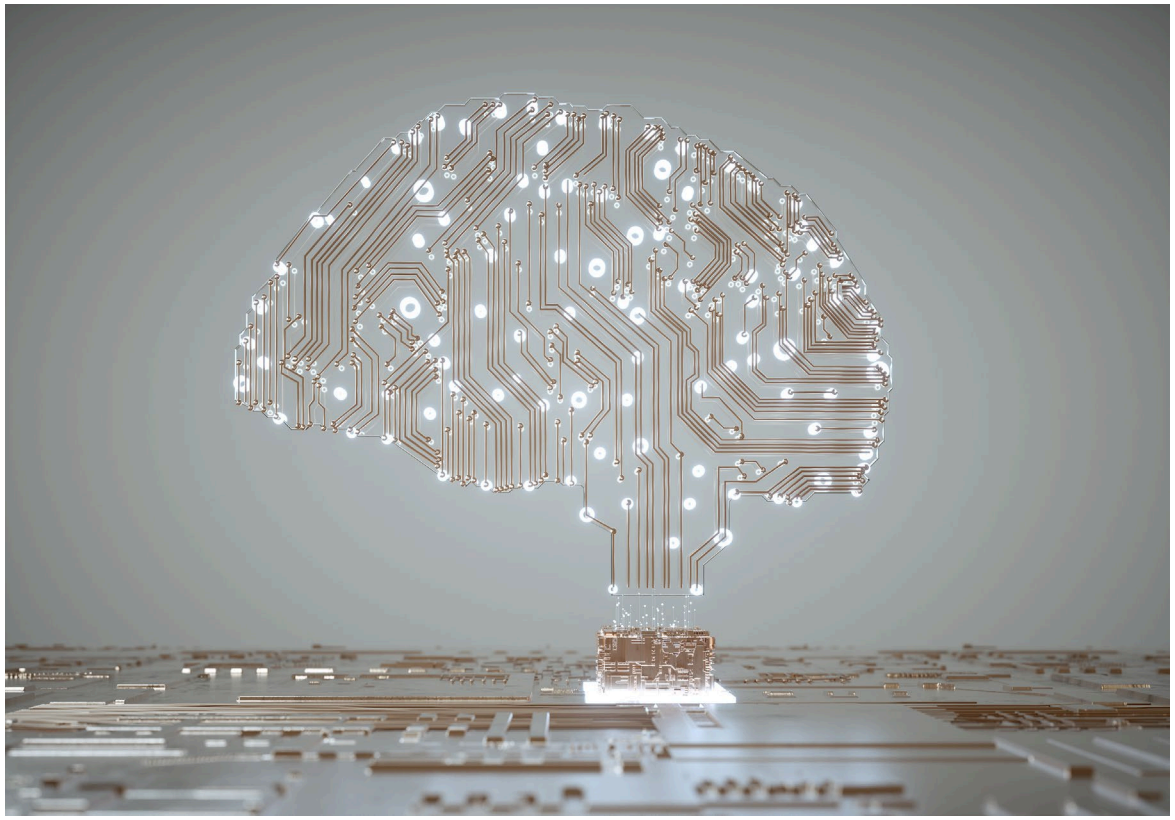
Current SOTA for MDSW that is also Health Software (SaMD)

Health Software

Part 1: General requirements for product safety

Areas covered:

- Health software product requirements
- Health software – Software life cycle processes
- **Health software product validation**
- Health software product identification and accompanying documents
- Post-market activities for the health software product



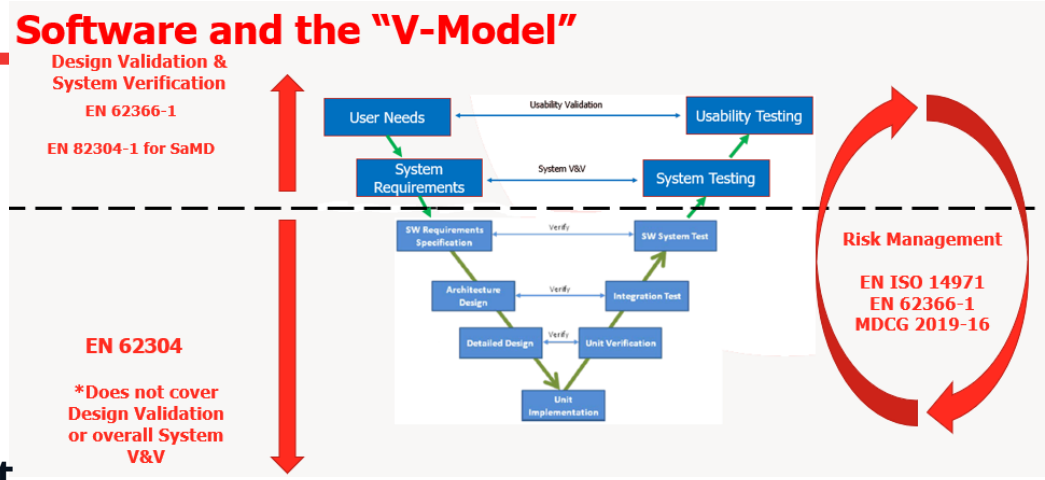
HEALTH SOFTWARE

Software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care

EN 82304-1:2017

Health Software Product Validation

Validation Plan → Validation Activities → Validation Report



Validation Plan
- Scope of activities
- Constraints
- Methods and acceptance criteria
- Operating environments, platforms
- Qualifications of personnel
- Independence from design team of personnel

Validation Activities
- Readiness

Plan established, Team established, Development phase complete
- Validation performed in intended environments, platforms with deviations justified

Validation Report
- Results of validation traceable to requirements (design inputs)
- Product meets use requirements
- Residual risk remains acceptable
- Validation conditions and results of validation activities
- List of anomalies
- Team members

Anomalies via Problem Resolution Process

Summary and Conclusion

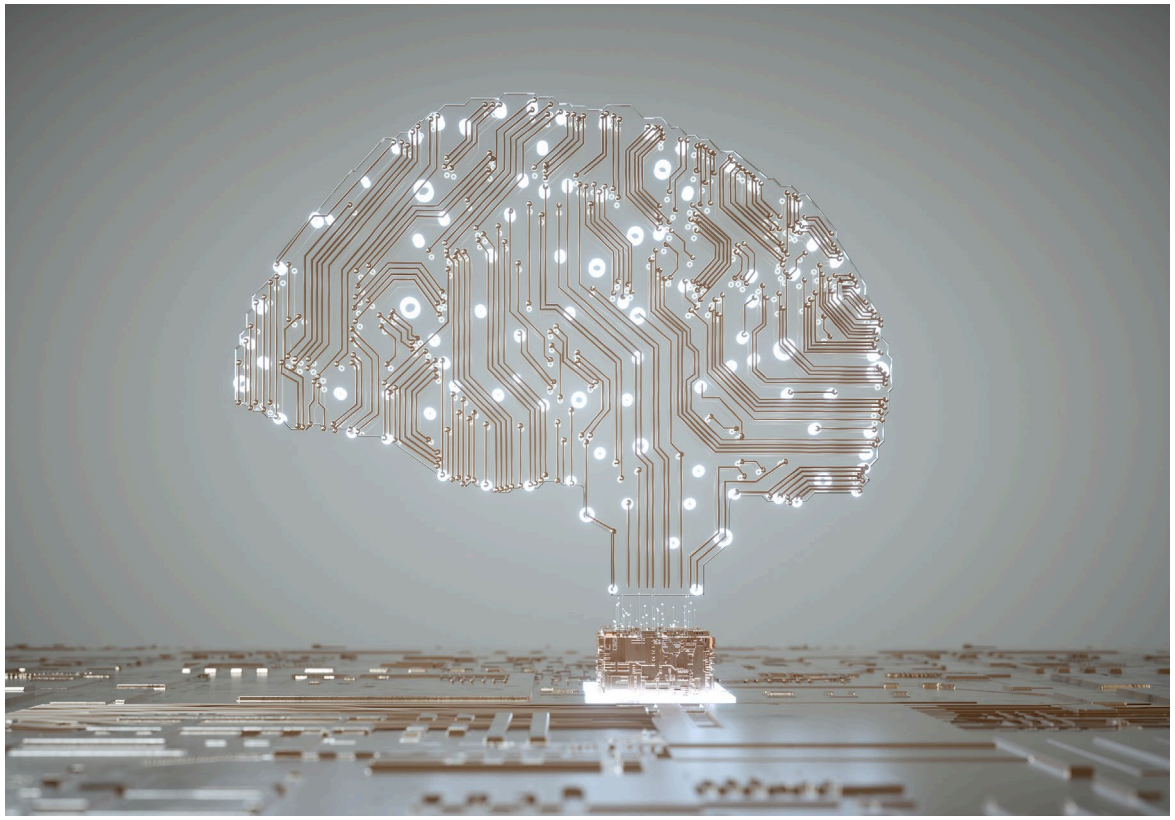
EN 62366-1:2015+A1:2020

Current SOTA for usability engineering for medical devices

Medical devices
Part 1: Application of usability engineering to medical devices

Areas covered:

- **Usability Engineering Process**
  - Use specification
  - UI characteristics related to safety/potential use errors
  - Hazard-related use scenarios for summative evaluation
  - User interface specification
  - Planning for formative, summative evaluations
  - UI design, implementation, formative evaluation
  - Summative evaluation
  - User Interface of Unknown Provenance (UOUP)



USABILITY
Characteristic of the USER INTERFACE that facilitates use and thereby establishes EFFECTIVENESS, EFFICIENCY and USER satisfaction in the intended USE ENVIRONMENT

bsi.

EN 62366-1:2015+A1:2020

- Has usability been addressed in the risk management file?
- Have formative and/or summative testing been conducted?
- If either formative and/or summative testing has not been conducted, has a valid rationale been provided? UOUP?
- Was testing conducted with representative users? (e.g. clinicians, lay users, etc. as per defines USER PROFILE)
- Are sample sizes/number of users tested appropriate?
- Are usability issues encountered during the usability engineering process tracked/dispositioned/implemented into the UI design appropriately?

Other standards may apply for a particular MDSW based on it's **Intended Purpose** or particular functional characteristics.

The standards just discussed are the most common ones that generally apply to all MDSW.

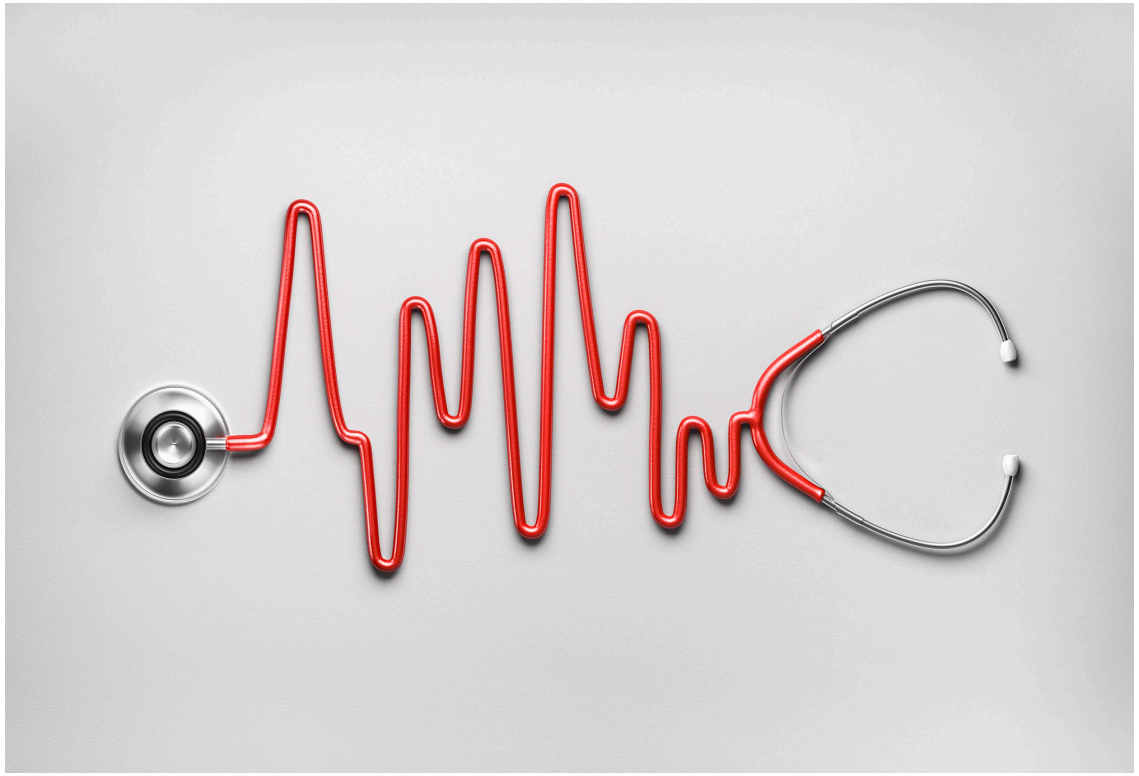
Important Guidance for MDSW

MDCG 2019-11

Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

Areas covered:

- **Scope is to understand if a particular software is considered "Medical Device Software" and thus regulated under MDR and/or IVDR**
- **Decisions steps for classification of MDSW under MDR**
- **Considerations for placing MDSW on the market and conformity assessment:**
  - As a medical device in its own right
  - As an integral component/part of a device
- **Application of IMDRF risk classification for MDR Rule 11**
- **Examples (MDSW and non-MDSW)**



Medical Device Software (MDSW)
Medical device software is software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a "medical device" in the medical devices regulation[15] or in vitro diagnostic medical devices regulation.[16]

15 Article 2(1) of Regulation (EU) 2017/745 – MDR
16 Article 2(2) of Regulation (EU) 2017/746 – IVDR

MDCG 2019-11

Is the SaMD classified properly under MDR Rule 11?

State of Healthcare situation or patient condition	Significance of Information provided by the MDSW to a healthcare situation related to diagnosis/therapy		
	High Treat or diagnose ~ *IMDRF 5.1.1*	**Medium** Drives clinical management ~ *IMDRF 5.1.2*	**Low** Informs clinical management *(everything else)*
Critical situation or patient condition ~ *IMDRF 5.2.1*	**Class III** *Category IV.i*	**Class IIb** *Category III.i*	**Class IIa** *Category II.i*
Serious situation or patient condition ~ *IMDRF 5.2.2*	**Class IIb** *Category III.ii*	**Class IIa** *Category II.ii*	**Class IIa** *Category I.ii*
Non-serious situation or patient condition *(everything else)*	**Class IIa** *Category II.iii*	**Class IIa** *Category I.iii*	**Class IIa** *Category I.i*

Table 1: Classification Guidance on Rule 11

No class I possible under this classification approach

Definitions of Significance of Information and State of Healthcare provided IMDRF/SaMD WG/N12FINAL:2014

MDCG 2021-24

Guidance on classification of medical devices.

Areas covered:

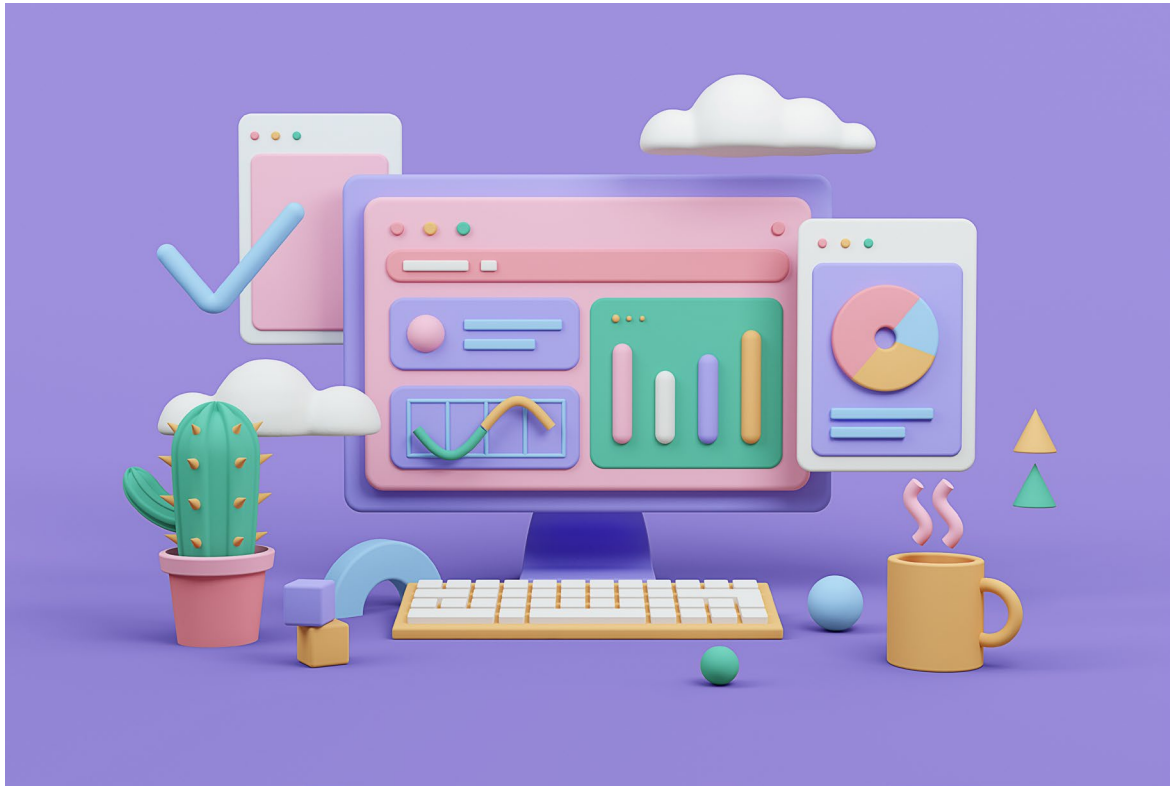
- Provides additional clarifications and examples of device classification under EU MDR (I, IIa, IIb, III)
- Provides some additional information and examples specific to Software devices against rule 11.
- Example of class I software provided

Class	Rule 11	Examples
IIa	Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:	• MDSW intended to rank therapeutic suggestions for a health care professional based on patient history, imaging test results, and patient characteristics, for example, MDSW that lists and ranks all available chemotherapy options for BRCA-positive individuals. • Cognitive therapy MDSW where a specialist determines the necessary cognitive therapy based on the outcome provided by the MDSW.
III	— death or an irreversible deterioration of a person's state of health[1], in which case it is in class III; or	• MDSW intended to perform diagnosis by means of image analysis for making treatment decisions in patients with acute stroke.
IIb	— a serious deterioration of a person's state of health[1] or a surgical intervention, in which case it is classified as class IIb.	• A mobile app intended to analyse a user's heartbeat, detect abnormalities and inform a physician accordingly. MDSW intended for diagnosing depression based on a score resulting from inputted data on patient symptoms (e.g. anxiety, sleep patterns, stress etc.).
IIa	Software intended to monitor physiological processes is classified as class IIa,	• MDSW intended to monitor physiological processes that are not considered to be vital. • Devices intended to be used to obtain readings of vital physiological signals in routine check-ups including monitoring at home.
IIb	except if it is intended for monitoring of vital physiological parameters[3], where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.	• Medical devices including MDSW intended to be used for continuous surveillance of vital physiological processes in anaesthesia, intensive care or emergency care.
I	All other software is classified as class I.	• MDSW app intended to support conception by calculating the user's fertility status based on a validated statistical algorithm. The user inputs
		(BBT) and menstruation days to track and predict ovulation. The fertility status of the current day is reflected by one of three indicator lights: red (fertile), green (infertile) or yellow (learning phase/cycle fluctuation).

MDCG 2021-24

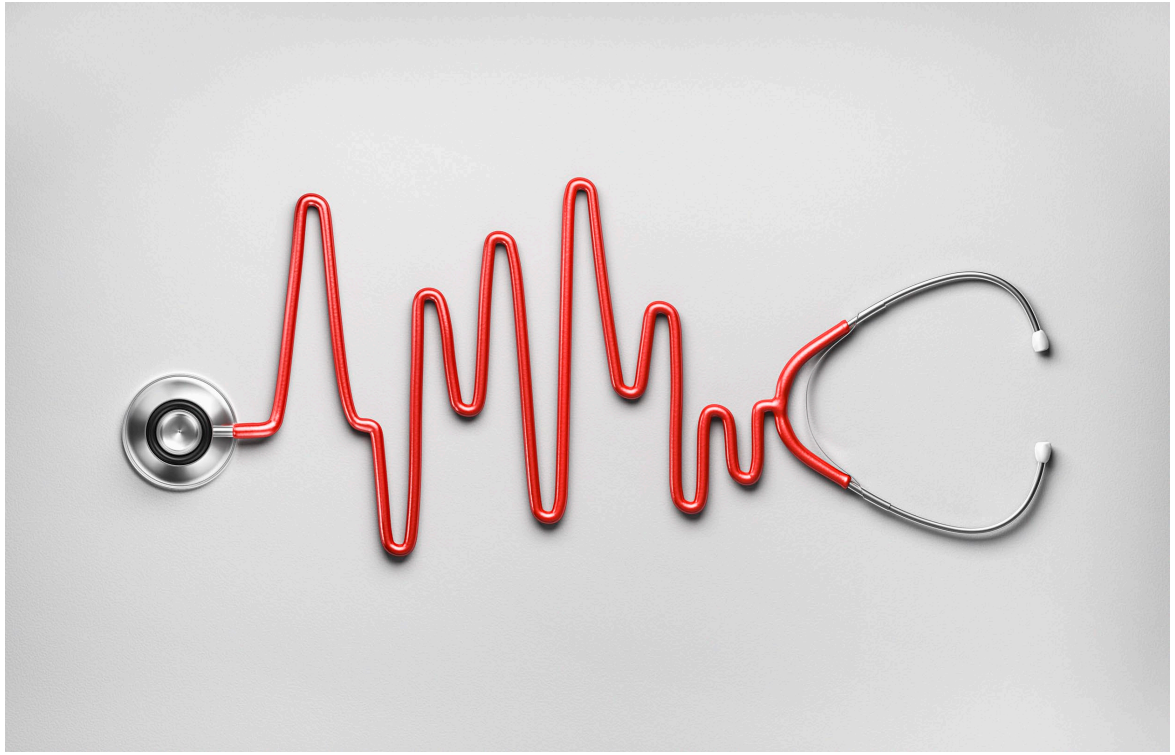
- **Rule 15** - Devices used for contraception or prevention of sexually transmitted diseases:
  - *Fertility monitors and **medical device software intended to be used in contraception (**e.g. by using the basal body temperature)'* ➔ **Class IIb**

- **Rule 9** - Active therapeutic devices intended to administer or exchange energy, as well as active devices intended to control/monitor/directly influence certain devices
  - *Programmer for: [IPG, ICD, Implantable Loop Recorder]* ➔ **Includes SW-only Apps** ➔ **Class III**
  - *Remote monitoring devices for active implantable devices* ➔ **Includes SW-only server/cloud devices for monitoring** ➔ **Class III**



MHRA - Medical device stand-alone software including apps (including IVDMDs)

- Guidance on qualification of software as Medical device or IVD Medical Device
- Clarifications on definitions: Software, accessory, system, modules, intended purpose
- Example of medical device software for diagnosis, monitoring, treatment, compensation.
- Guidance on classification, Essential Requirements, PMS and labelling
- Annexes:
  - Symptom checkers
  - Clinical calculators
  - ‘Drives or influences the use of a device’
  - Field Safety Warnings and End-of-Life notification



MHRA - Medical device stand-alone software including apps (including IVDMDs)

Key Points

- **Annex IX Classification, implementing rule 2.3, guidance**

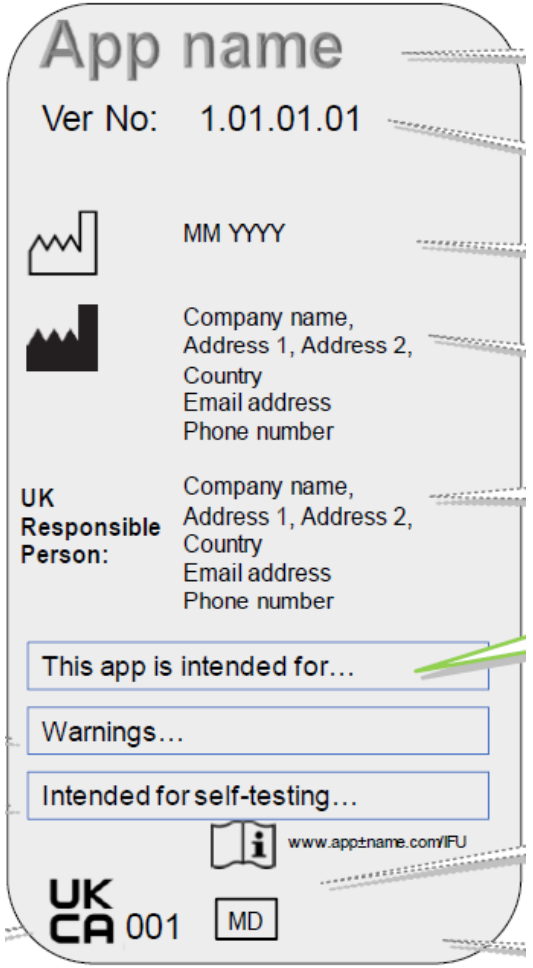
'Software that directly modifies the state/action/use of another device is considered to be driving that device.'

'Software which produces data that is intended to be manually fed into a device, thereby modifying the state/action/use of the device, is considered to be influencing that device.'

'The term "drives a device or influences the use of a device" can include anything from direct control of a device to just selecting a device. This must be an intended action by the manufacturer of the software and not just an accidental influence on use of a device'

- **Annex IX rule 10, 'direct diagnosis'**

'A device is considered to "allow direct diagnosis" when:
- it provides the diagnosis of the disease or condition by itself,
- it provides decisive information for making a diagnosis, or
- claims are made that it can perform as, or support the function of, a clinician in performing diagnostic tasks.
For devices intended to be used by lay users, provision of an indicative diagnosis may be enough to imply that the device is allowing direct diagnosis.'



A prospective buyer should be able to identify that the app meets the relevant essential requirements prior to purchase. As such, a developer should display the UKCA mark on the primary landing page and as a screen shot in any app store.

MDCG 2019-16

Guidance on Cybersecurity for medical devices:

Areas covered:

- Introduction/Objectives/Trace to requirements in Regulations
- Basic Cybersecurity Concepts
- Secure Design and Manufacture
- Documentation and Instructions for use
- Post-Market Surveillance and Vigilance
- Other Legislation and guidance

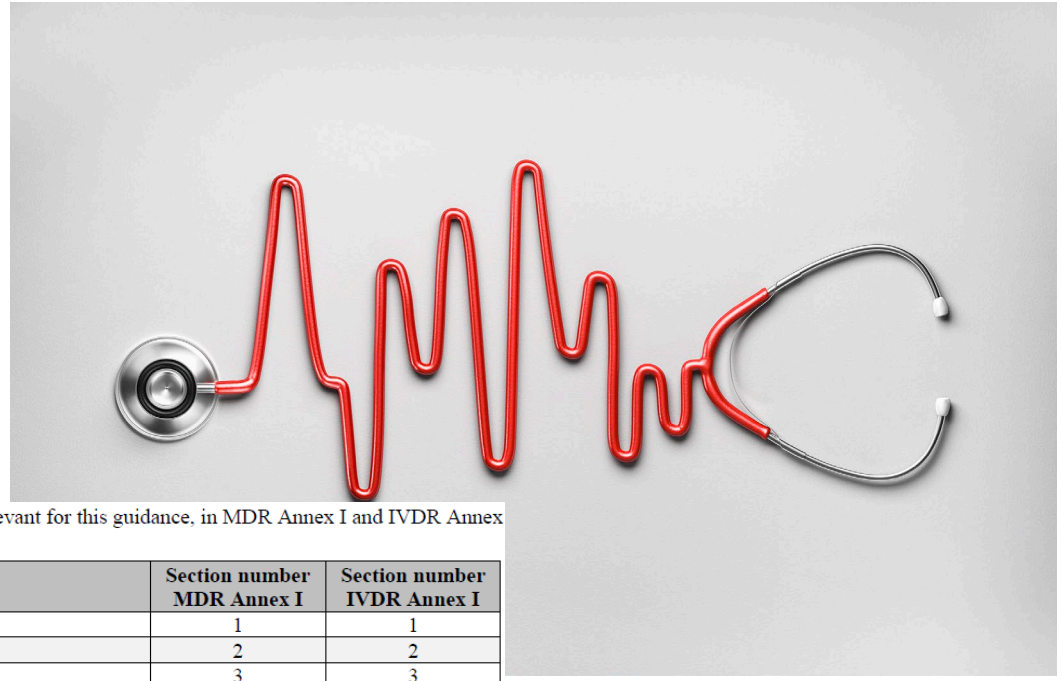


Table 1: Correspondence table between sections, relevant for this guidance, in MDR Annex I and IVDR Annex I

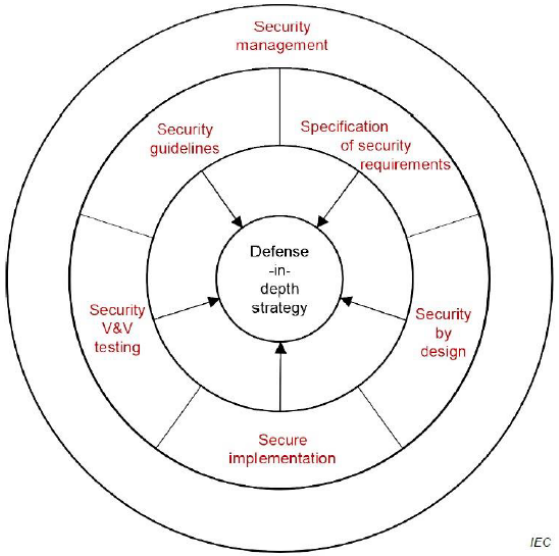
Main topic	Section number MDR Annex I	Section number IVDR Annex I
Device performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
Combination/connection of devices/systems	14.1	13.1
Interaction between software and the IT environment	14.2.d	13.2.d
Interoperability and compatibility with other devices or products	14.5	13.5
Repeatability, reliability and performance	17.1	16.1
Development and manufacture in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation	17.2	16.2
Minimum IT requirements	17.4	16.4
Unauthorised access	18.8	-
Lay persons	22.1	-
Residual risks (information supplied by the manufacturer)	23.1 g	20.1 g
Warnings or precautions (information on the label)	23.2 m	20.2 m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4 g	-
Minimum IT requirements (information in the instructions for use)	23.4.ab	20.4.1.ah

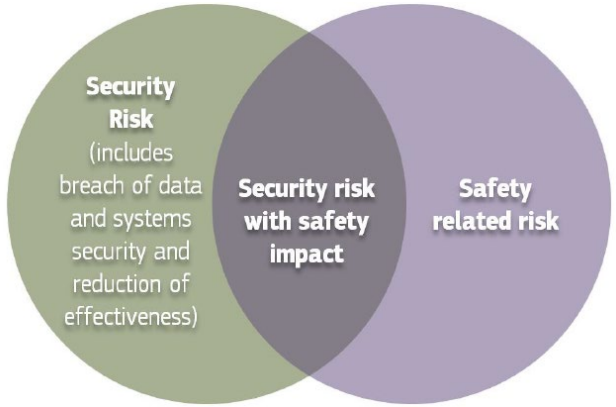
MDCG 2019-16

Key Points

The Notified Body will want to know:

- Is security integrated with the development and risk management processes? ➔ **Should not be "bolted on" at the end!**
- Is there a security risk management plan?
- Is there a security risk assessment? ➔ Should minimally consider threats to Confidentiality, Availability, Integrity
- Has security-focused V&V testing been conducted? E.g.:
  - Security feature testing
  - Fuzz testing
  - Vulnerability scans
  - Penetration testing
- Are security mitigations captured in requirements?
- Are necessary IT/security requirements established in the IFU?
- Does the PMS/Vigilance process incorporate vulnerability and security incident monitoring ➔ Common Vulnerabilities and Exposures
- How are security updates & patches applied to SW in the field?

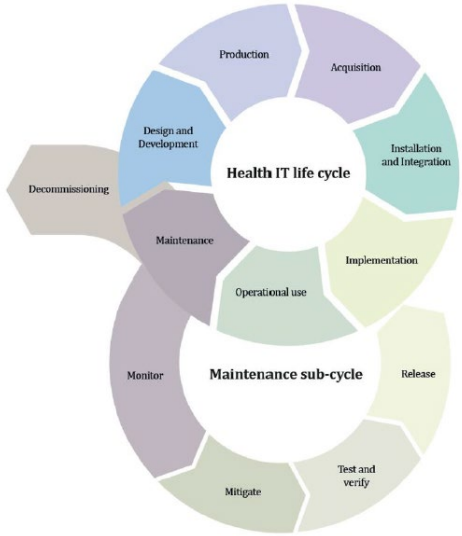


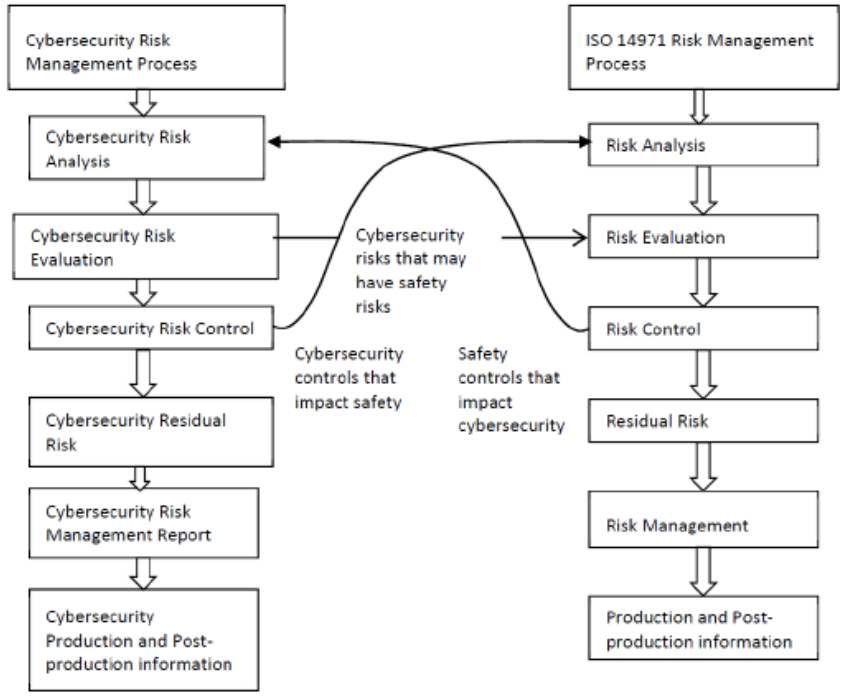


MDCG 2019-16

Key Points (cont'd)

- Cybersecurity risk management can affect safety risk management (and *vice versa*)
- Both processes should include monitoring in the post-production phase to identify elevated risks and take appropriate action when needed.
- Cybersecurity risk assessment should be updated based on information from the post-production phase.
- Patches/updates to address security concerns could be in the MDSW itself or in SOUP components (operating system, libraries, etc.)





MDCG 2020-1

Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software

Areas covered:

- General principles of MDSW clinical / performance evaluation process – Introduction
- Determination of the clinical association / scientific validity
- Technical Performance / Analytical Performance
- Clinical Performance
  - Clinical investigations and clinical performance studies
  - When conformity based on clinical data is not deemed appropriate
- Final analysis and conclusion
- Continuous update of the CER/PER

CLINICAL INVESTIGATION (MDR)
Any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device.

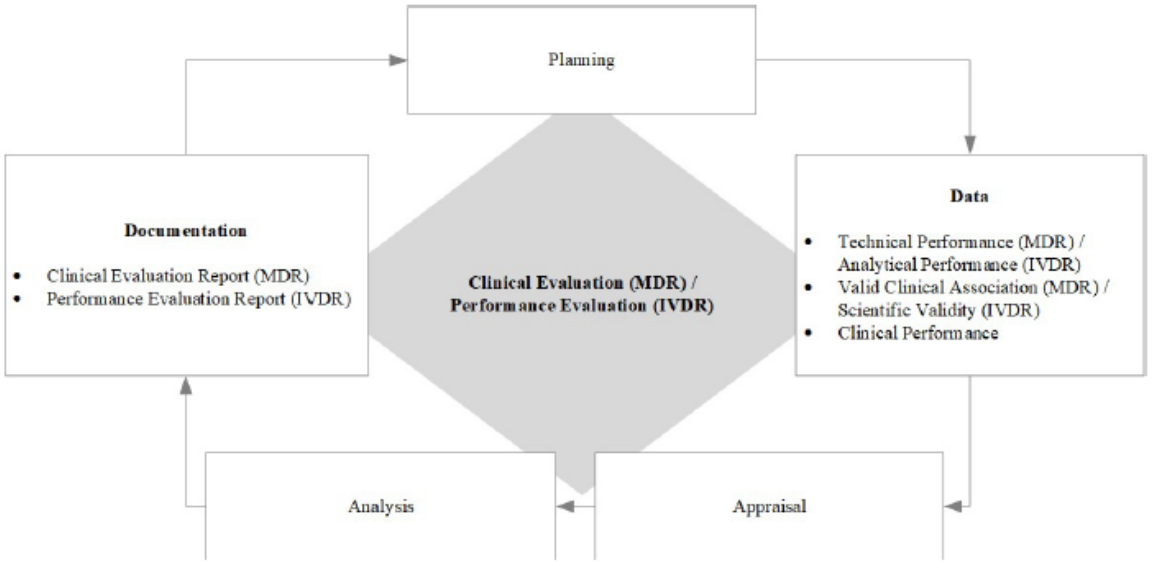
PERFORMANCE STUDY (IVDR)
An assessment and analysis of data to establish or verify the SCIENTIFIC VALIDITY, the ANALYTICAL and, where applicable, the CLINICAL PERFORMANCE of a device.

bsi.

MDCG 20201

Key Points

- What clinical investigations / performance studies have been conducted to support the claims made for the MDSW?
- Where equivalence is claimed, is the equivalence analysis appropriate?
  - Clinical equivalence (Same)
  - Technical equivalence (Similar)
- Is state-of-the-art appropriately considered and documented in the CER?
  Should consider other available treatments / diagnostic solutions (not just similar devices)
- Are the pre-clinical performance testing and validation (including usability) adequately described



No difference in clinical evaluation expectations just because the device is a software device.

(see also MEDDEV 2.7/1 Rev. 4)

MDCG 2018-5

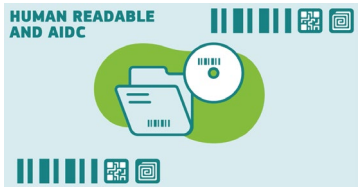
UDI Assignment to Medical Device Software

Areas covered:

- Scope of UDI requirements for software
- Basic UDI-DI
- Changes to UDI-DI
- Minor software revisions
- Evaluation of changes to software by manufacturers
- UDI Placement Criteria

NOTE: UDI placement criteria for software are laid down in Annex VI, Part C, point 6.5.4 of the MDR and Annex VI, Part C, point 6.2.4 of the IVDR

MDCG 2018-5



Key Points

- How is the **UDI-PI** displayed / communicated by the software?
  - For SW with a UI, often this can be on a regulatory information / 'about' screen

- Are appropriate processes in place to update the **UDI-DI** when necessary? From the guidance:
  It can therefore be concluded that, in the specific case of software,
  - *Any change of the Basic UDI-DI*
  - *Any changes which impact the original performance, safety, or the interpretation of data*
  - *A change to the name or trade name, version or model number, critical warnings or contra-indications, user interface language*

  *would require a new **UDI-DI**.*

MDR Annex VI, Part C, point 6.5.4 / IVDR Annex VI, Part C, point 6.2.4:

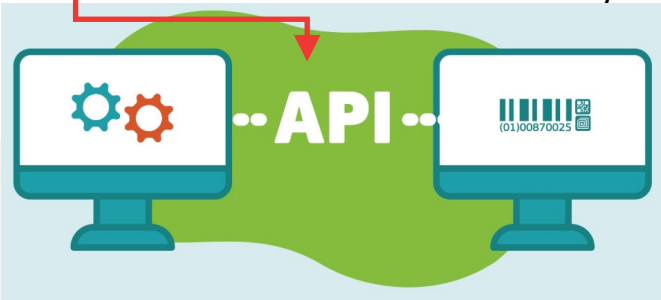
a) each packaging level shall bear the human readable and AIDC representation of the complete UDI. The UDI that is applied to the physical medium containing the software and its packaging shall be identical to the UDI assigned to the system level software;

b) the UDI shall be provided on a readily accessible screen for the user in an easily-readable plain-text format, such as an 'about' file, or included on the start-up screen;

c) software lacking a user interface such as middleware for image conversion, shall be capable of transmitting the UDI through an application programming interface (API);

d) only the human readable portion of the UDI shall be required in electronic displays of the software. The marking of UDI using AIDC shall not be required in the electronic displays, such as 'about' menu, splash screen etc.;

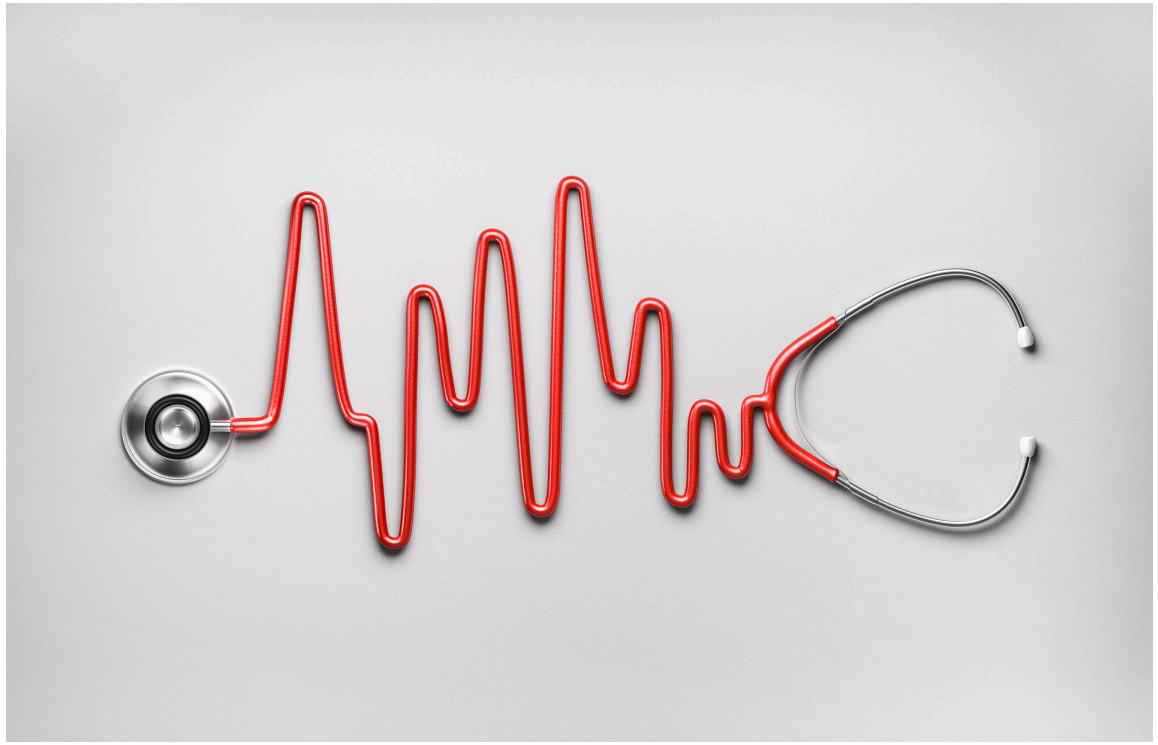
e) the human readable format of the UDI for the software shall include the Application Identifiers (AI) for the standard used by the issuing entities, so as to assist the user in identifying the UDI and determining which standard is being used to create the UDI.



Medical Device Software (MDSW) – Hardware combinations

Areas covered:

- Regulatory considerations for combination of software with hardware or hardware components.
- scenarios treated:
  - External hardware component providing input data to a MDSW app
  - Hardware component incorporated within a smartphone or wearable connected to a MDSW app
  - Legal manufacturer of HW and MDSW is the same entity
  - Legal manufacturers of HW and MDSW are different entities

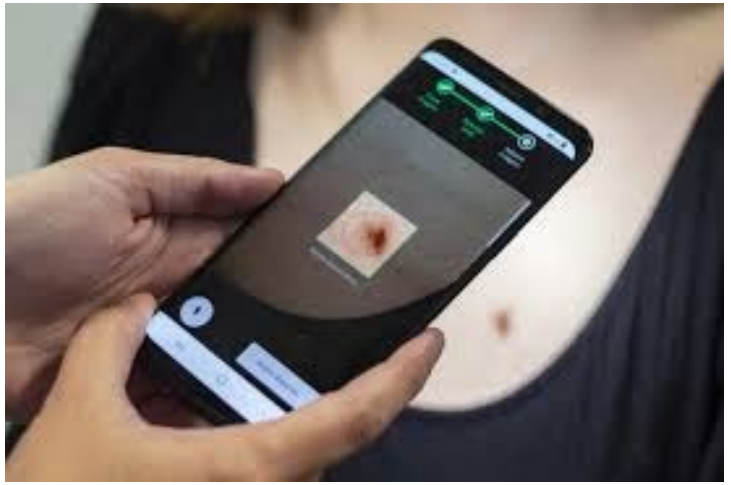


MDCG 2023-4

Key Points

Option 3: the hardware or hardware component is an integral part of a general consumer product or wearable digital product and **is not a medical device or an accessory to a medical device** and has no intended medical purpose.

In option 3, the MDSW manufacturer is not able to rely on the compliance and conformity of the hardware or hardware component with the MDR. In this case, it is not sufficient to verify the safety, performance, reproducibility, interoperability and compatibility. Moreover, the MDSW manufacturer becomes responsible for the safety, performance and reproducibility of the hardware or hardware component in its combined use with the MDSW in all intended configurations. The MDSW manufacturer must comply with the requirements under equivalent conditions to a situation where a manufacturer is combining a medical device with another product according to Article 22(4).7



Other guidance can also be consulted to ensure SOTA coverage for SaMD:

- IMDRF/SaMD WG/N12FINAL:2014 – “Software as a Medical Device”: Possible Framework for Risk Categorization and Corresponding Considerations
- FDA - Content of Premarket Submissions for Device Software Functions
- FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- FDA - Postmarket Management of Cybersecurity in Medical Devices
- AAMI TIR57 - Principles for medical device security—Risk management
- AAMI TIR97 - Principles for medical device security—Postmarket risk management for device manufacturers **…** Any many others **with more to com**e…

Clinical Evaluation of MDSW

Clinical Evaluation guidance specific to MDSW

Identification of two kinds of SW groups

a) Software for which the manufacturer claims a specific medical intended purpose. Such software has a CLINICAL BENEFIT and requires CLINICAL EVIDENCE within its own conformity assessment.

b) Software for which the manufacturer does not claim any medical intended purpose. Such software is intended to drive or influence a medical device. The CLINICAL EVIDENCE is provided within the context of the driven or influenced device. (...and is therefore out of the scope of this document.)

If the device under review is SW which drives a system, though the MDCG states it is out of scope it goes on to immediately identify types of clinical assessments which can be done with this SW.

MDCG 2020-1 Considerations.

What level of influence are you?

Evidence may be comprised of 3 items depending on the level of influence.

1) SaMD which has its own clinical benefits, must have its own clinical evidence.
2) SaMD which drives a system may have data from itself and the system, or
3) the system of its own accord independent of the otherwise invisible SW which drives it.

SW either way must-have clinical data in support of the entry to the market. SW which is invisible to the end user but drives the end results is very likely to have direct or related clinical benefits. This driving of other devices do not allow the device under review to escape Article 61 requirements.

Model of Software	**CLINICAL EVALUATION** (MDR) / **PERFORMANCE EVALUATION** (IVDR) **- scope**
MDSW (with independent intended purpose and claimed CLINICAL BENEFIT)	MDSW only
MDSW (with intended purpose and claimed CLINICAL BENEFIT related to driving or influencing a medical device for a medical purpose)	MDSW and the driven or influenced medical device Notes 1,2
Software driving or influencing the use of a medical device (with no independent intended purpose or independent claimed CLINICAL BENEFIT)	Driven or influenced medical device including the software (component or accessory)

MDR Article 61(10)

What it is:

- Bench testing. Preclinical data. Verification and validation tests.

- “Without prejudice to paragraph 4, where the demonstration of conformity with general safety and performance requirements based on clinical data is not deemed appropriate, adequate justification for any such exception shall be given based on the results of the manufacturer's risk management and on consideration of the specifics of the interaction between the device and the human body, the clinical performance intended and the claims of the manufacturer. In such a case, the manufacturer shall duly substantiate in the technical documentation referred to in Annex II why it considers a demonstration of conformity with general safety and performance requirements that is based on the results of non-clinical testing methods alone, including performance evaluation, bench testing and pre-clinical evaluation, to be adequate”

When you may use it:

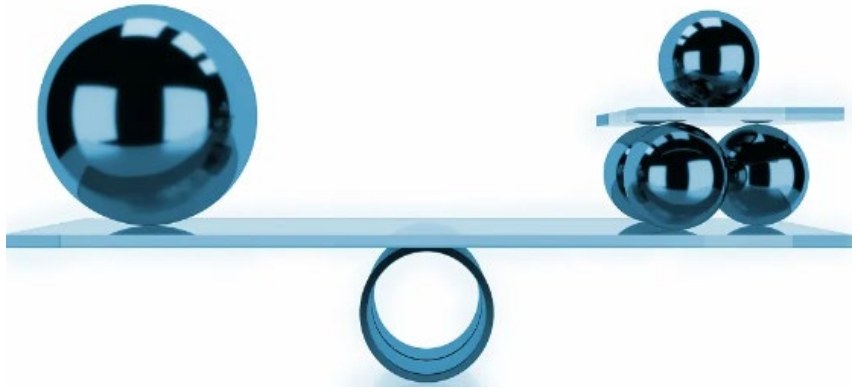
It can be difficult for SaMD to follow 61 (10):

- Clinical Performance and intended purpose are present. SaMD has some specific clinical performance/benefits that are meaningful and measurable to the patient.
- Previous Talks given by BSI’s Global Head of Clinical Compliance, Richard Holborow, have already been given on this topic.
- This is stated here briefly as more SW devices make the attempt to approach the clinical assessment by this route than any other device type.
- Not unique to MDSW Article 61(10) is reserved for entry to market, and or unethical or impossible clinical evidence. This is a high bar. Far less than 1/100 devices reviewed by BSI are actually 61(10), more than 15 % are attempted to be 61(10).

Assume you are likely not 61(10).

Equivalence

- “…The notified body shall, in circumstances in which the clinical evidence is based partly or totally on data from devices which are claimed to be equivalent to the device under assessment, assess the suitability of using such data, taking into account factors such as new indications and innovation. The notified body shall clearly document its conclusions on the claimed equivalence, and on the relevance and adequacy of the data for demonstrating conformity…”

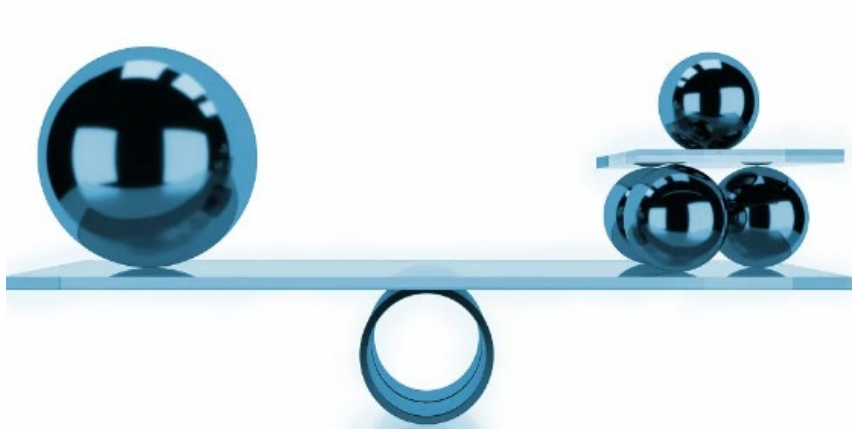


Equivalence

- Consider using the equivalence table per MDCG 2020-5 Annex I.

- Technical characteristics 'It is the functional principle of the software algorithm, as well as the clinical performance(s) and intended purpose(s) of the software algorithm, that shall be considered when demonstrating the equivalence of a software algorithm. It is not reasonable to demand that equivalence is demonstrated for the software code, provided it has been developed in line with international standards for safe design and validation of medical device software.

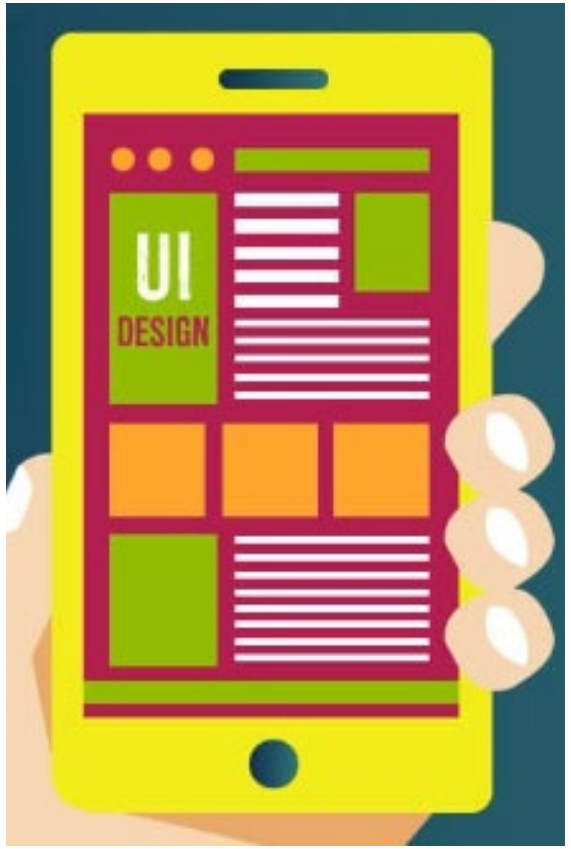
- 'Software solely intended for the configuration of a device (e.g. presentation on a graphical user interface etc), and not related to any medical purpose14 (e.g.diagnosis, treatment etc), does not need to be similar when considering equivalence as long as it can be justified to not negatively affect the usability, safety or clinical performance.



MDR, Annex XIV Part A (3)	MEDDEV 2.7/1 rev 4, Appendix A1
The device is of similar design; is **used under similar conditions of use**; has similar specifications and properties including physicochemical properties such as intensity of energy, tensile strength, viscosity, surface characteristics, wavelength and **software algorithms**; uses similar deployment methods, where relevant; has similar principles of operation and critical performance requirements.	- be of similar design, and - **used under the same conditions of use**, and - have similar specifications and properties (e.g. physicochemical properties such as type and intensity of energy, tensile strength, viscosity, surface characteristics, wavelength, surface texture, porosity, particle size, nanotechnology, specific mass, atomic inclusions such as nitrocarburising, oxidability), and - use similar deployment methods (if relevant), and - have similar principles of operation and critical performance requirements

Equivalence

- Equivalence between SW requires to also consider equivalence of the user interface in technical characteristics.
- Usability impacts the kinds of errors possible.
- Usability impacts the compliance of a devices use.
- Usability impacts the way in which end users understand data on a screen and how they will interpret this.
- Having the same information is not inherently equality. A detailed assessment of what is displayed and how must be considered.



Clinical Benefits

SW device appear to uniquely suffer from ill-defined clinical benefits and clinical performance.

- Validation of the CLINICAL PERFORMANCE is the demonstration of a MDSW's ability to yield clinically relevant output in accordance with the intended purpose. The clinical relevance of a MDSW's output is a **positive impact**:
- on the health of an individual expressed in terms of measurable, **patient-relevant clinical outcome(s), including outcome(s) related to diagnosis, prediction of risk, prediction of treatment response**(s), or
- related to its function, such as that **of screening, monitoring, diagnosis or aid to diagnosis of patients**, or
- on patient management or public health: reduced time to treatment/diagnosis

Clinical Benefits

To find your benefit consider the following questions and exercises.

- Who benefits from my device?
- What benefit does my device confer to users and patients?
- Where in the hospital or outpatient system is my device used and where is that benefit most obvious?
- When in the work stream of the procedures being undertaken does my device fit, and when is that benefit realized?
- Why is my device of benefit?
- How is my device of benefit?

Clinical Benefits

The answer to these and similar questions will help legal manufacturers to identify what the benefit is for the device.

- If the device under review did not exist, what benefits are lost?
- Who do your indications for use serve?
- What is the best possible clinical facing outcome for the device under review?
- If the device under review were to be pulled from the market tomorrow, who suffers? Why?
- What claim would your marketing team love to make about outcomes?
- If the device were used on you, why are you happy about that?

Clinical Benefits

- If you arrive at benefits, for each of these items consider the further questions of “How would I prove it?”

Enough Data / Enough Performance to Support the Benefit

- When do you have enough evidence?
- When do you have enough performance defined to support the benefit?

Evidence: How many performance claims support the benefit? How many legs does a table have?

This is a table

This is a table

This is a table

This is a table

Enough Data / Enough Performance to Support the Benefit

When do you have enough evidence? When do you have enough performance defined to support the benefit?

When you have enough legs to stand on. Think of the table top as the claims and benefits made. A sufficient number of legs must exist to support both the number and weight of the claims made. There is no magic rule, but SaMD devices tend to miss in the following ways…

Enough Data / Enough Performance to Support the Benefit

- SW claims to improve the patient outcomes by informing the users of state XYZ. Informing alone is not supporting this statement. Evidence must show patient outcomes.
- SW claims to improve patient compliance to a medical regimen. Evidence of alarms and indicators are not evidence. Improved patient compliance must be demonstrated.
- SW claims to better enable clinicians to monitor patients for disease states XYZ. Telling the physician is not evidence. Improves sensitivity or specificity of specific clinical prognosis diagnosis or management recommendations must be demonstrated.

Enough Data / Enough Performance to Support the Benefit

- SW claims to improve the doctors workflow by displaying XYZ all in one place, reducing time to decision making. Displaying this information is not evidence. Evidence must show reduced time to decision making, (Without clinically significant increase in errors!)
- Remember SW has safety claims too!
- SW claims to reduce time to treatment of patients by means of displaying XYZ…You guessed it. Evidence of reduced time to treatment is required.

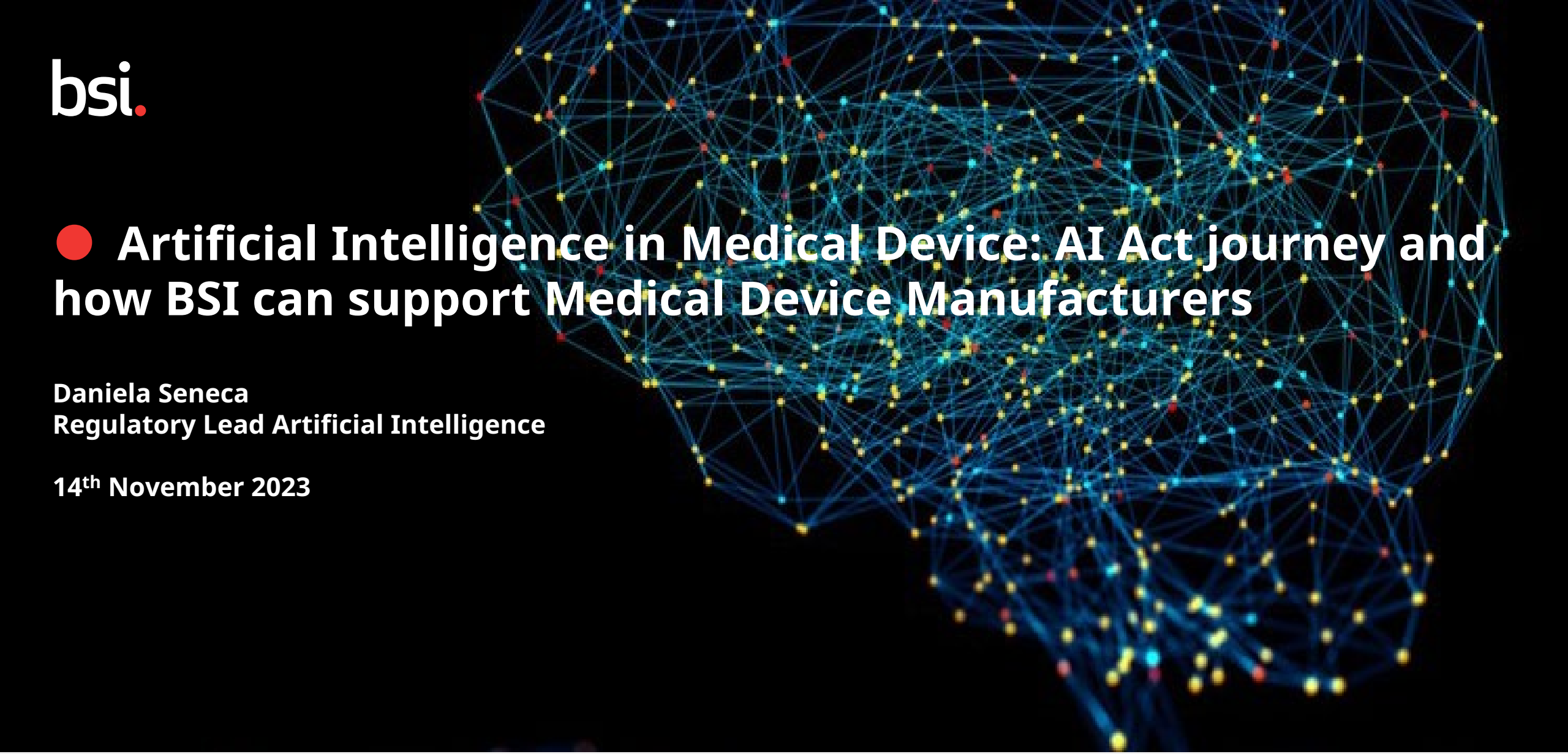
Enough Data / Enough Performance to Support the Benefit

- Support your table top of claimed and clinical benefits, with enough performance rationale and data!

Any question?

Have a short break

The webinar will restart in



Artificial Intelligence in Medical Device: AI Act journey and how BSI can support Medical Device Manufacturers

Daniela Seneca
Regulatory Lead Artificial Intelligence

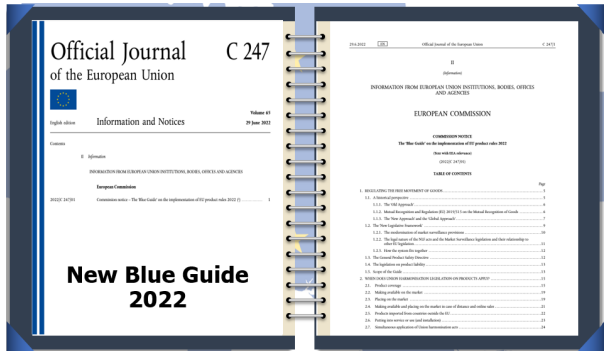
14th November 2023

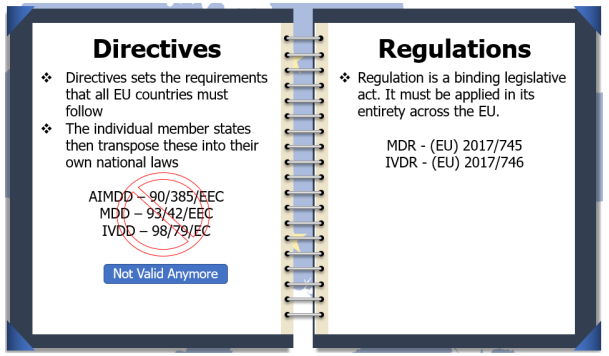
Agenda

- Introduction & Welcome
- The AI Act
- BSI approach
- Group discussion

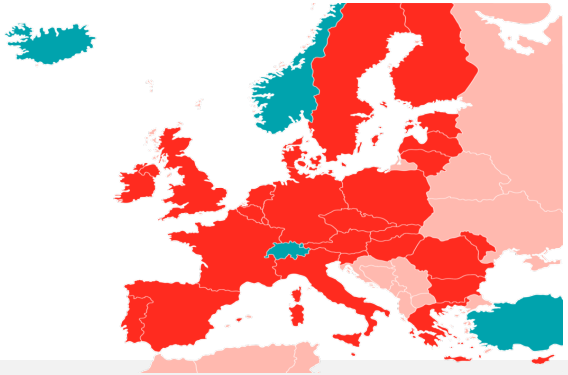
Introduction & Welcome

Medical Device Conformity Assessment – New Legislative Framework



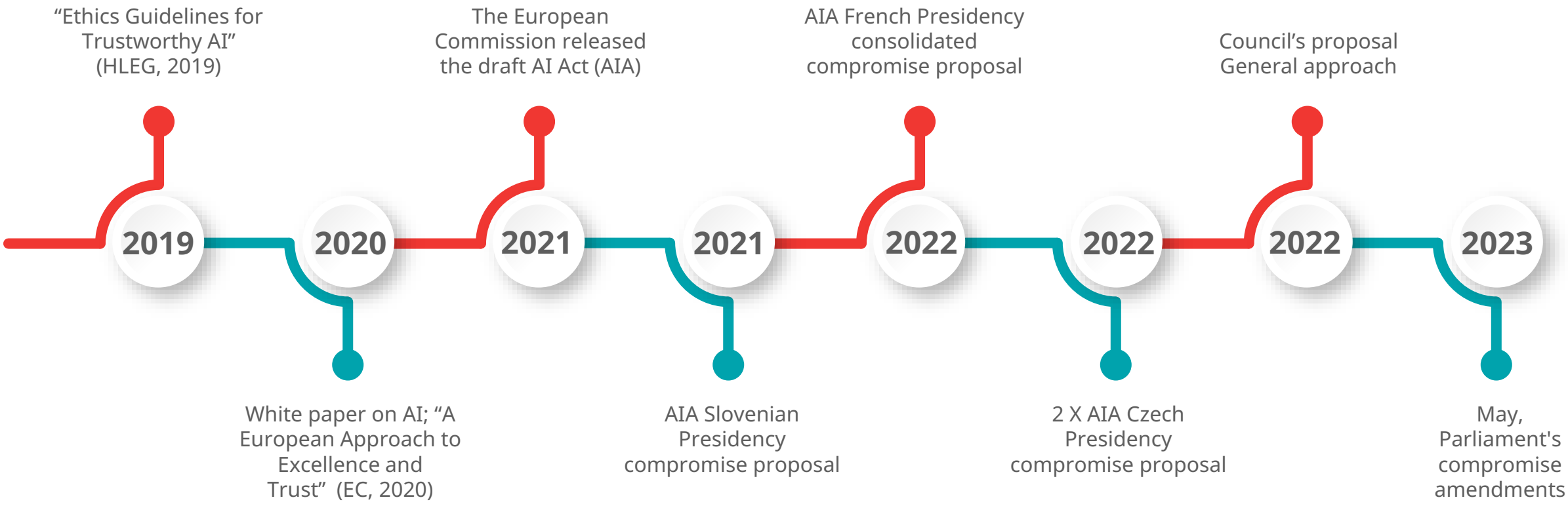


Medical Device? → Classify the device → Select Conformity Assessment Route → **3rd Party Conformity Assessment** → CE Certification → Sign Declaration of Conformity → Affix CE Mark → Post-Market Surveillance

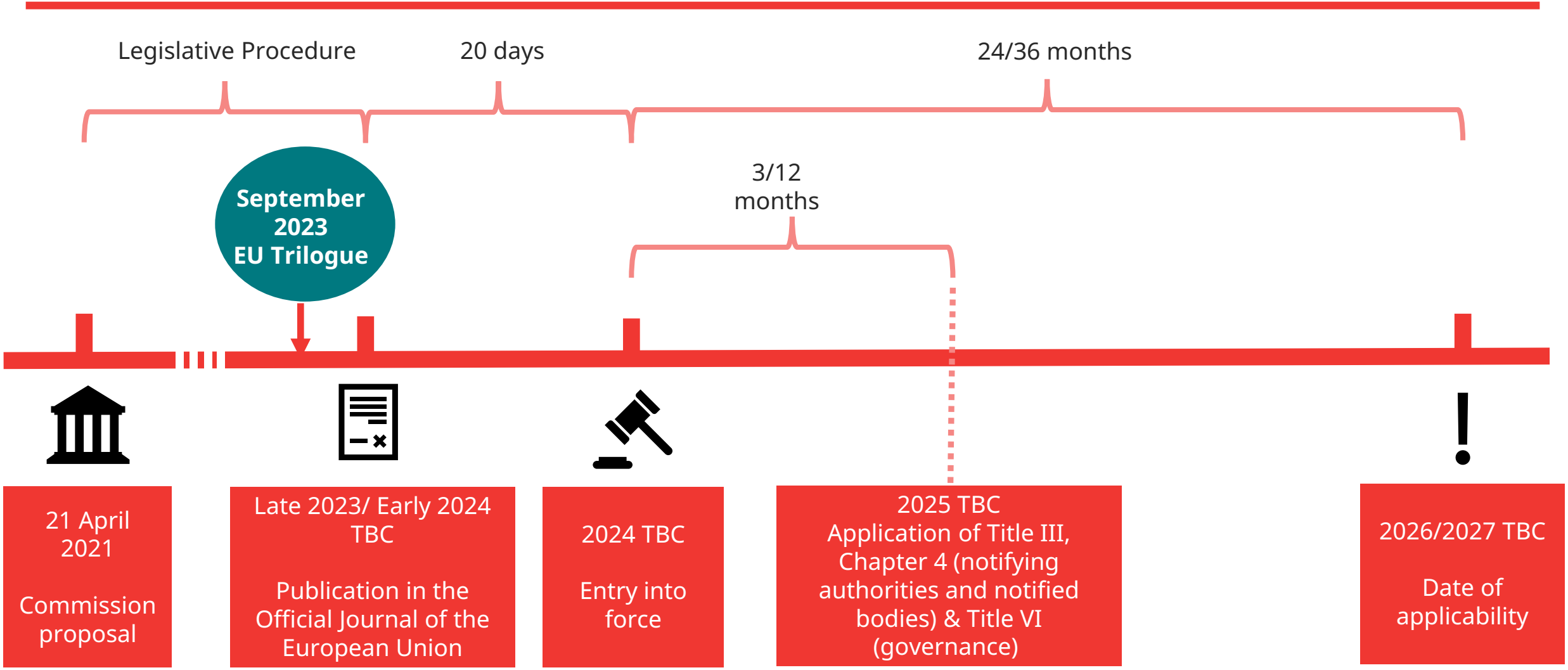


https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.notifiedbody&dir_id=34

AI Act Journey



EU AI Act Outlook



The Artificial Intelligence Act

Council of the European Union
General Secretariat

Brussels, 29 June 2023

WK 8800/2023 INIT

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Artificial Intelligence Act – 4-column document

Delegations will find in annex the 4-column document concerning the AI Act.

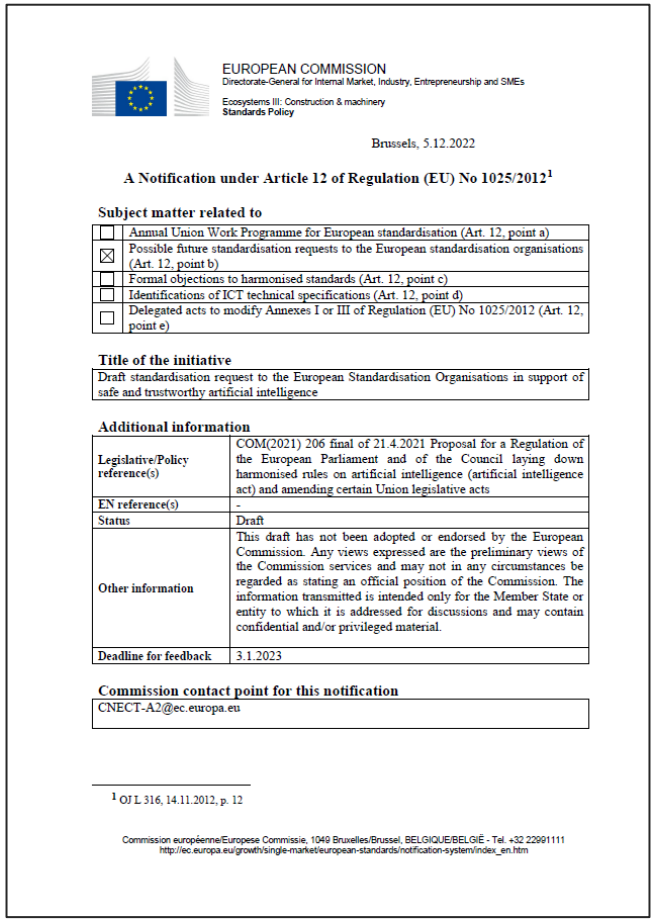
Artificial Intelligence System - definition

	Commission Proposal	EP Mandate	Council Mandate
126	Article 3 Definitions	Article 3 Definitions	Article 3 Definitions
Article 3, first paragraph			
127	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:
Article 3, first paragraph, point (1)			
128	(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;	(1) 'artificial intelligence system' (AI system) means ~~software~~*a machine-based system* that is ~~*developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined*~~*designed to operate with varying levels of autonomy and that can, for explicit or implicit* objectives, generate outputs such as ~~*content,*~~ predictions, recommendations, or decisions*, that influence physical or virtual environments* ~~*influencing the environments they interact with*~~;	(1) 'artificial intelligence system' (AI system) means ~~*software*~~*a system* that is ~~*developed with one or more of the techniques and approaches listed in Annex I and can, for*~~*designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve* a given set of ~~*human-defined objectives, generate*~~*objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated* outputs such as content *(generative AI systems)*, predictions, recommendations~~,~~ or decisions*,* influencing the environments ~~*they interact with*~~*with which the AI system interacts*;

Engineered System that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

- BS EN ISO/IEC 22989:2023

Standardization Request



EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Ecosystems III: Construction & machinery
Standards Policy

Brussels, 5.12.2022

A Notification under Article 12 of Regulation (EU) No 1025/2012[1]

Subject matter related to

☐	Annual Union Work Programme for European standardisation (Art. 12, point a)
☒	Possible future standardisation requests to the European standardisation organisations (Art. 12, point b)
☐	Formal objections to harmonised standards (Art. 12, point c)
☐	Identifications of ICT technical specifications (Art. 12, point d)
☐	Delegated acts to modify Annexes I or III of Regulation (EU) No 1025/2012 (Art. 12, point e)

Title of the initiative

Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence

Additional information

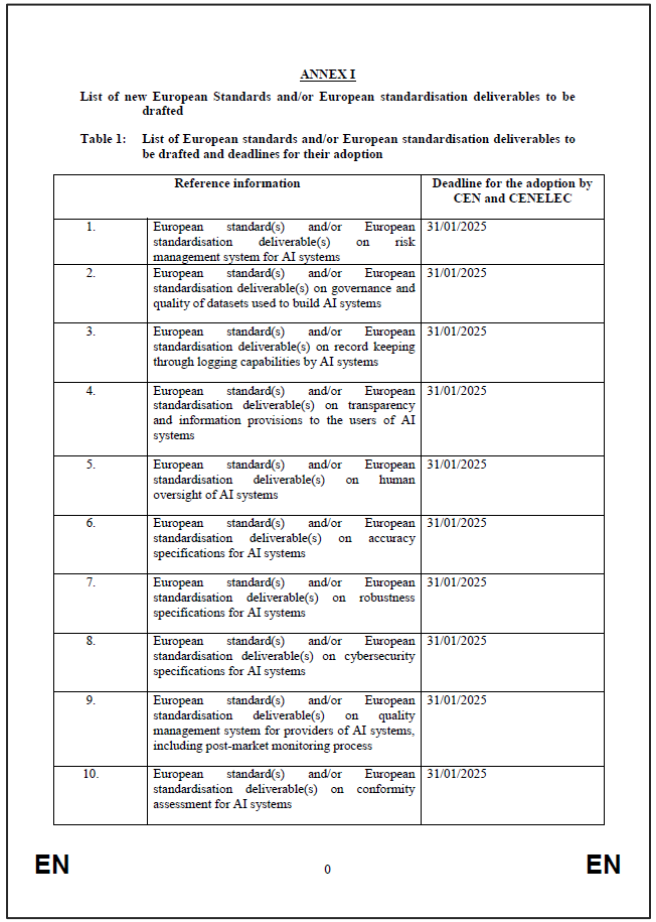
Legislative/Policy reference(s)	COM(2021) 206 final of 21.4.2021 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts
EN reference(s)	-
Status	Draft
Other information	This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and may contain confidential and/or privileged material.
Deadline for feedback	3.1.2023

Commission contact point for this notification

CNECT-A2@ec.europa.eu

[1] OJ L 316, 14.11.2012, p. 12

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
http://ec.europa.eu/growth/single-market/european-standards/notification-system/index_en.htm



ANNEX I

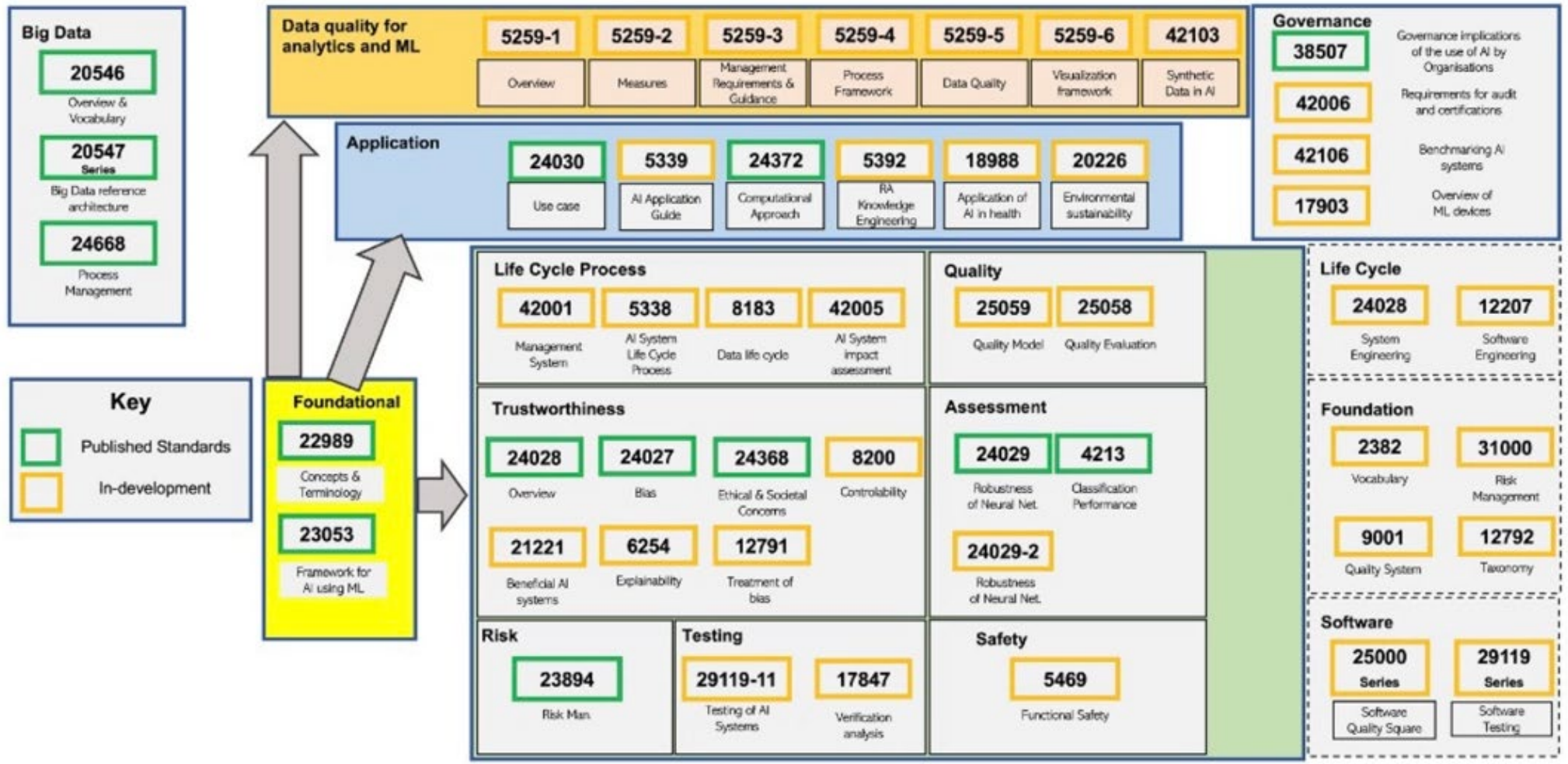
List of new European Standards and/or European standardisation deliverables to be drafted

Table 1: List of European standards and/or European standardisation deliverables to be drafted and deadlines for their adoption

	Reference information	Deadline for the adoption by CEN and CENELEC
1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems	31/01/2025
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems	31/01/2025
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems	31/01/2025
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems	31/01/2025
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems	31/01/2025
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems	31/01/2025
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems	31/01/2025
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems	31/01/2025
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process	31/01/2025
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems	31/01/2025

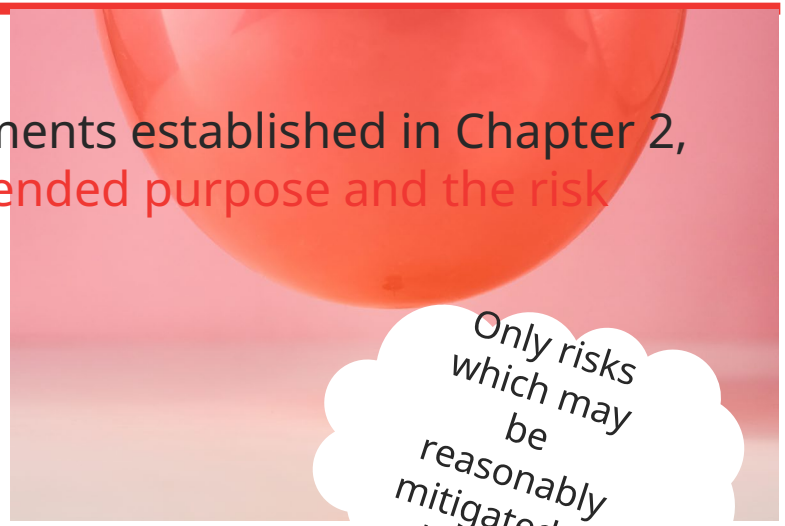
EN 0 EN

AI standards map



Chapter 2: Requirements for high-risk AI systems

The AI Act requires the high-risk AI systems to comply with the requirements established in Chapter 2, taking into account the generally acknowledged state of the art, the intended purpose and the risk management system.



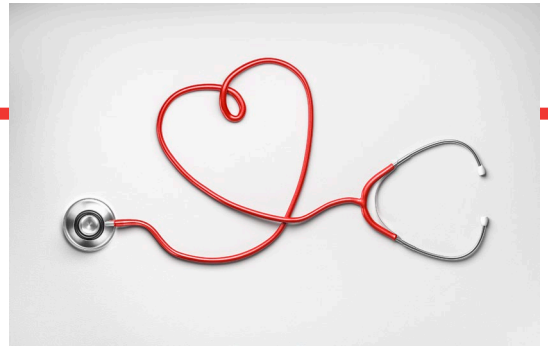
Article 9 – Risk management system

1. Shall be established, implemented, documented and maintained.

2. Shall be understood as a continuous iterative process planned and run throughout the entire lifecycle, requiring regular systematic updating. It shall comprise the following steps:

a) Identification and analysis of the known and foreseeable risks to health, safety and fundamental rights
b) Evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system
c) Adoption of suitable risk management measures

Chapter 2: Requirements for high-risk AI systems



Article 9 – Risk management system

The risk management measures shall

3. Give due consideration to the effects and possible interaction resulting from the combined application of the requirements, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

4. Be such that any residual risk associated with each hazard as well as the overall residual risk is judged acceptable. In identifying the most appropriate risk management measures, the following shall be ensured:

a) elimination or reduction of risks identified and evaluated as far as possible through adequate design and development
b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated
c) provision of adequate information and, where appropriate, training to users

considering the user's technical knowledge, experience, education, training and the environment in which the system is intended to be used.

Chapter 2: Requirements for high-risk AI systems

Article 10: Data and data governance

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria.

2. Data governance practices shall concern

- Design choices
- Data collection processes
- Data preparation processing operations as annotation, labelling, cleaning, enrichment and aggregation
- Relevant assumptions on information that the data are supposed to measure
- **Prior assessment** of the availability, quantity and suitability of the needed data sets
- Biases affecting health and safety or leading to discrimination
- Data gaps or shortcomings

Chapter 2: Requirements for high-risk AI system

(EU) 2021/222 6 on eIFU?

Article 13: Transparency and provision of information to users

Shall be designed and developed to ensure sufficiently transparent operation, achieving compliance with the relevant obligations and enabling users to understand and use the system appropriately. It shall be accompanied by instructions for use (IFU) in an appropriate digital format or otherwise including concise, complete, correct and clear information, relevant, accessible and comprehensible to users.

IFU shall specify

- Identity and contact details of provider and, where applicable, authorised representative
- Characteristics, capabilities and limitations of performance: intended purpose (including geographical, behavioural or functional settings), accuracy (and its metrics), robustness and cybersecurity and any circumstances impacting them, misuse, behaviour regarding specific persons, specifications for input data, description of expected output
- Changes
- Human oversight measures for output interpretation
- Computational and hardware resources needed, lifetime, maintenance, maintenance frequency, updates
- Description of mechanism for users to properly collect, store and interpret logs

Chapter 2: Requirements for high-risk AI system

Article 14: Human oversight

- High-risk AI designed to be effectively overseen by natural persons
- Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights
- Human oversight shall be ensured through “pre” built-in measures (by the provider) and “post” measures (identified by the provider but implemented by the user)
- Human oversight enabled to understand capacities and limitations, automation bias, system’s output, override or reverse the output, interrupt the system.
- For remote biometric identification systems: 2 natural persons separate verification and confirmation

Article 16: Obligations of providers

- Ensure compliance to requirements
- Indicate name, address on the system or on packaging or on accompanying documentation
- Have a compliant quality management system (QMS)
- Keep the required documentation
- Keep the logs generated by the system
- Ensure the system undergoes the relevant conformity assessment procedure (Annex VI or VII)
- Comply with registration obligation
- Inform national competent authorities and notified body of non-compliance and corrective actions
- Affix CE marking
- Demonstrate conformity upon a national competent authority request

Article 20 Automatically generated logs

Providers shall keep the logs for at least 6 months unless provided otherwise.

Financial institutions included.

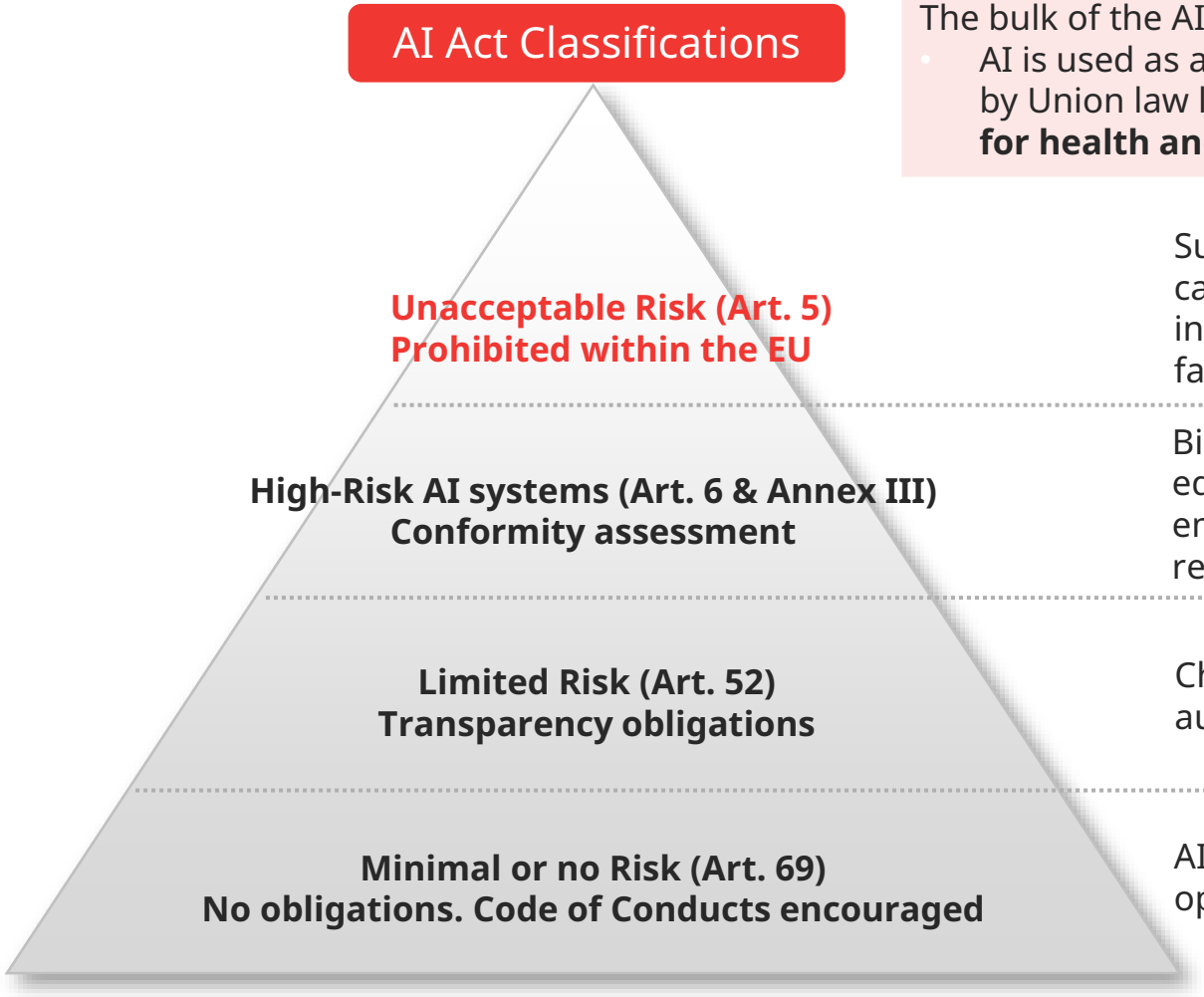
A risk-based approach

Unacceptable Risk (Title II, Article 5)	Prohibited within the EU
High-Risk (Title III, Article 6)	Conformity Assessment - full application of Harmonised Standards and applicable Common Specifications
Limited Risk (Title IV, Article 52)	Transparency obligations
Minimal or no Risk (Title IX, Article 69)	Codes of Conduct (encouraged)

A risk-based approach

Requirements get stricter as the risk increases.
The bulk of the AI Act pertains to **high-risk AI systems:**

- AI is used as a safety component of a product / AI system is itself a product + covered by Union law listed in Annex II + **3rd party conformity assessment related to risks for health and safety +** AI systems listed in Annex III.



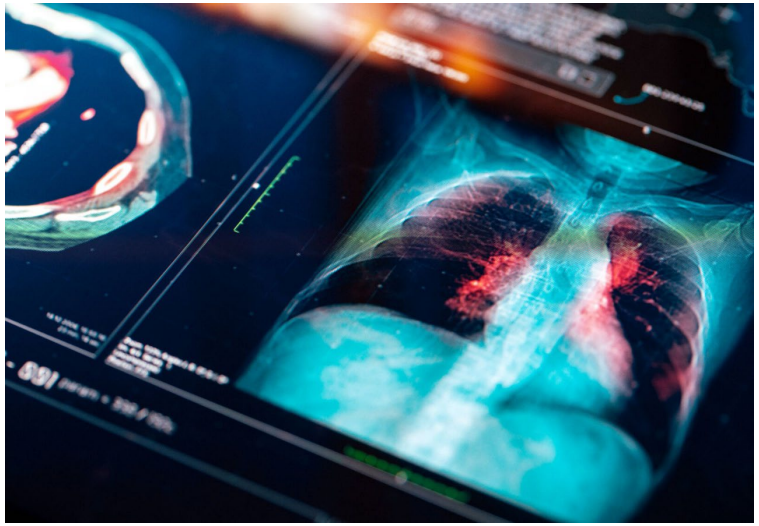
Subliminal techniques, exploiting vulnerabilities, biometric categorisation, social scoring, real time remote biometric identification in publicly accessible spaces, risk assessment of persons, scraping of facial images for facial recognition databases, infer emotions

Biometric identification (confirmation excluded), critical infrastructure, education and training, employment, essential services, insurance, emergency, law enforcement, migration, justice. Additional list to be reviewed annually (art. 84)

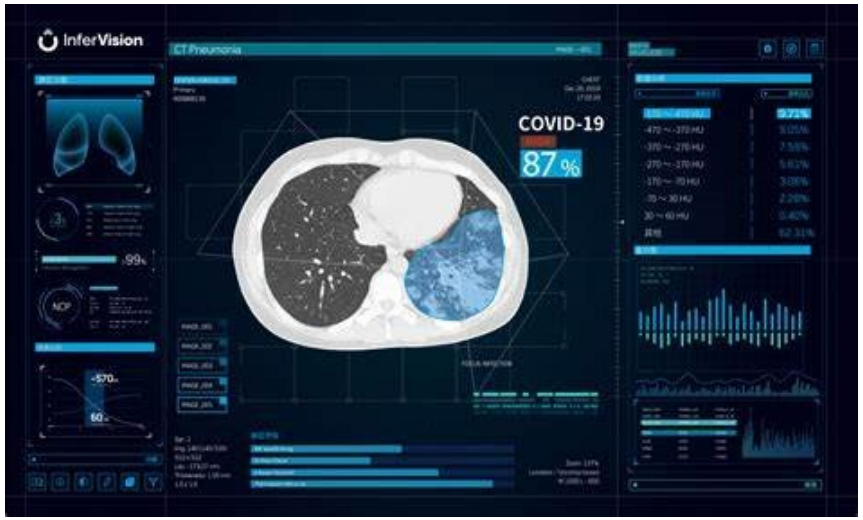
Chatbots, Biometric categorisation systems, emotion recognition, (text audio or visual content) deep fake.

AI-enabled videogames, spam filters, predictive maintenance, process optimisation

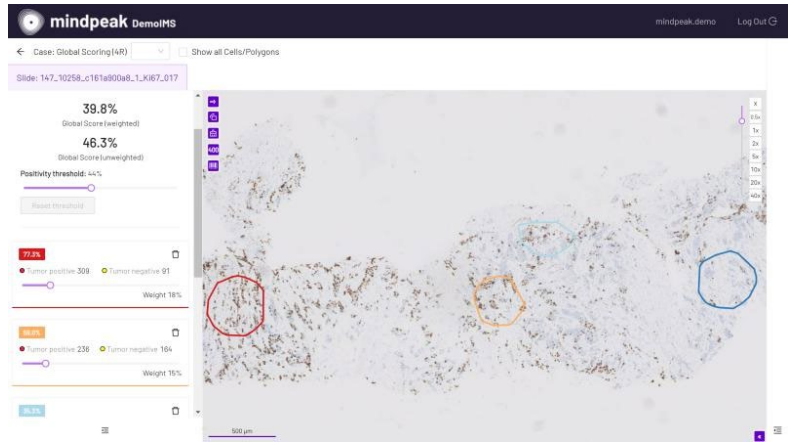
Examples of High-Risk AI Systems



Detection of cancerous lesions based on growing repositories of images



Detection of COVID-19 from lung CT scans



Automated scoring for cancer detection

AI Conformity Assessment

The AI Act requires providers of high-risk AI systems to conduct a **conformity assessment** before placing them on the EU market.

Annex II:
AI systems under Union harmonisation legislation (e.g., MDR/IVDR)

AI providers should ensure the accomplishment of the required conformity assessment under Union harmonisation law **(+)** the requirements set out in Chapter 2, Title III of the AI Act

A **single EU declaration of conformity** may be drawn up in respect of all Union legislations applicable to the high-risk AI system (+) a **single CE marking** will also indicate conformity with other legislations

As long as the requirements of the AI Act are addressed by Union harmonisation law, those requirements shall be deemed fulfilled

Notified bodies which have been notified under those Union harmonisation laws shall be entitled to perform conformity assessments against the requirements of the AI Act

bsi.

MD/IVD & AI Conformity Assessment

Is third party conformity assessment required for the medical device/in vitro device with AI component under MDR/IVDR (e.g. class IIa, IIb or III medical devices)?

The requirements of the AI Act should be assessed as part of the conformity assessment already foreseen under MDR/IVDR by the MDR/IVDR Notified Body

The medical device manufacturer will go through a **single conformity assessment** under the MDR *(lex generalis*), also considering the AI Act *(lex specialis)* requirements.

Single technical documentation, single declaration of conformity, single CE marking

BSI approach to forthcoming legislation

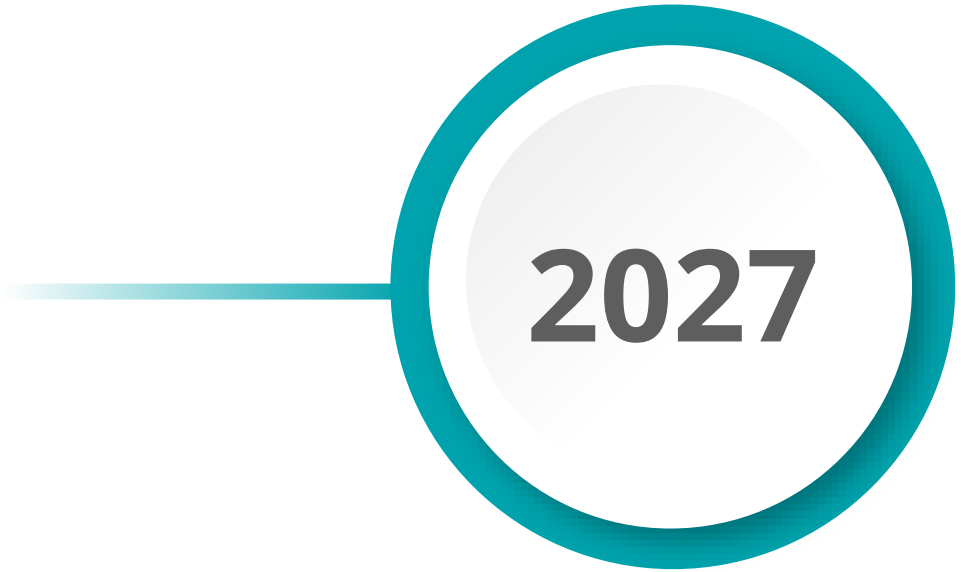
AI is expected to have a considerable impact on MD/IVD industry with various applications ranging from precision and personalised medicine to medical imaging and patient monitoring.

bsi.

CE 2797

BSI approach to forthcoming legislation

BSI is promoting a **proactive approach** to the upcoming regulation in order to help AI providers **anticipate requirements** and seamlessly adopt **habits of excellence** without stifling innovation



BSI approach to forthcoming legislation

MD/IVD AI components review

2023

The state of the art in AI has evolved, and continues to do so, with an increasing and more evident associated risk.

Given this and the applicable MDR/IVDR requirements, a team of **AI experts will undertake a technical documentation assessment** specifically for the AI components of the device.

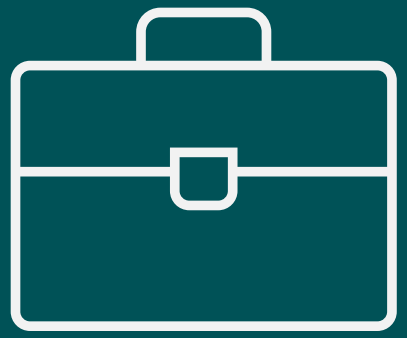
2027

BSI's Approach to AI Enabled Medical Devices*

One for all!

MDR/IVDR Conformity Assessment + Requirements from the AI Regulation

Audit of Quality Management System



Assessment of the Technical Documentation

AI Model(s) Verification by the Notified Body

Launching upon official publication of the AI Regulation on the OJEU

*Subject to change based on legislative requirements

MD/IVD AI components review

2023

Tools & developing/ deployment environment

- Description of **tools, methods and environment for developing and deployment** of AI/ML model(s)

Datasets

Requirements and metrics for:

- **Performance** (+ metrics)
- **Robustness** (+ metrics)
- **Development, testing & deploy environment**
- **Transparency**

AI/ML Verification and Validation

- **Data quality**, pre-processing, cleaning, channel effects, augmentation, bias analysis & mitigation,
- **Partitioning methods** (training/testing/validation)
- Datasets **annotation/ labelling methods**
- **Methods for training, testing and re-training**
- **V&V reports/evidence**

2027

AI trainings on AI standards

2023

A full understanding of the rapidly-changing AI regulation panorama **is critical for success.**

BSI is working to build and share **expertise** on AI fundamental principles including **fairness, bias and robustness,** enhanced by the **partnership with Citadel AI** for of AI compliance testing based on standards, **assuring safety and reliability of AI systems.**

2027

NOW AVAILABLE

ISO/IEC TR 24029-1:2021 - Assessment of the robustness of neural networks

Building trust in AI-enabled products

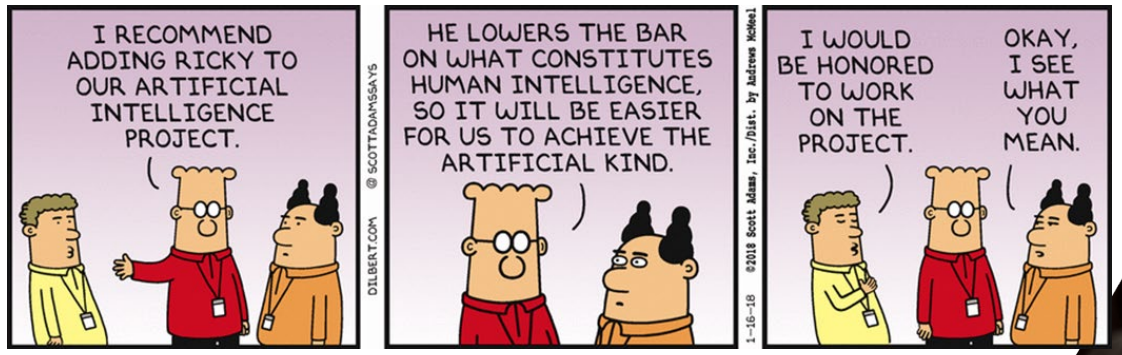
“Inspiring trust for a more resilient world”

Our **missions** is to share knowledge, innovation and best practice to help people and organizations **make excellence a habit.**

Our **vision** is to turn standards and best practice into habits of excellence, enabling organizations to reduce risks whilst **not stifling innovation.**

bsi.

Group discussion – Q&A



Thank you!

Contact us

Flavien Del Sole
Senior Business Development Manager
+33 6 35 81 41 24
Flavien.delsole@bsigroup.com