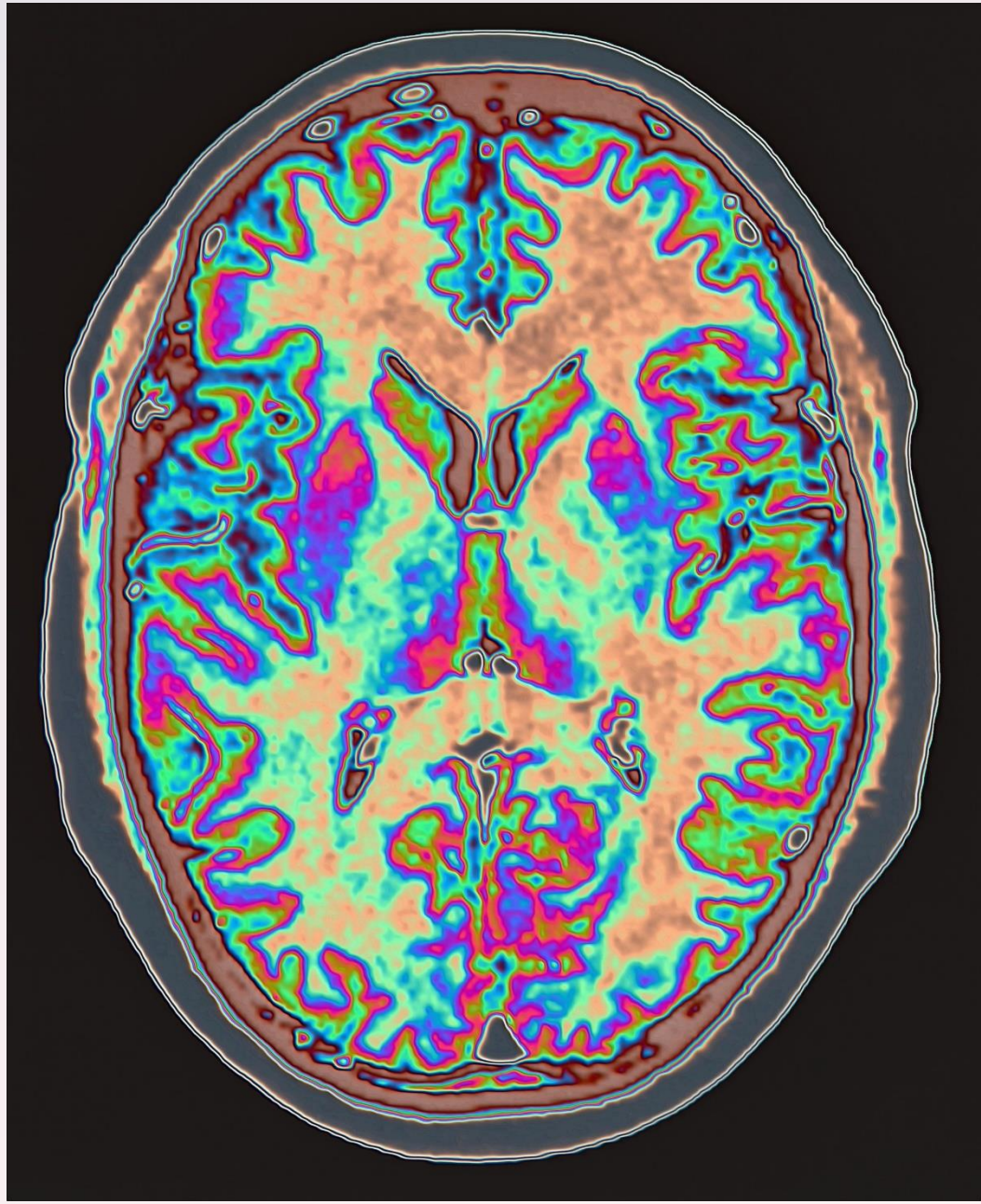
Understanding IVDR Software and Cybersecurity.

31 October 2023

Liz Harrison
Global Head of IVD

Thomas Doerge
Global Head Active Implantable Medical Devices, BSI



IVDR Classification of Software

IVDR Article 2 – definitions

Ensure your software meets the definition of an IVD medical device - ***MDCG 2019-11: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR***

IVDR Annex VIII – Implementing Rules

1.4 Software, which drives a device or influences the use of a device, shall fall within the same class as the device.
If the software is independent of any other device, it shall be classified in its own right.

IVDR Classification of Software – Key Consideration

Intended Purpose of the Software is key!

Software driving or influencing the use of an IVD instrument

- Tube position and pipetting
- Incubation times and temperature
- Optics
- Turning the instrument data into human readable result format

➢ **Classified with the IVD instrument intended purpose**

Software influencing clinical interpretation of results from specific IVD reagents

- Interrogating a genetic database per NGS variant calling files to associate the data with an inherited genetic disease
- Mobile App to replace human reading of results from a specific brand of lateral flow self-test

➢ **Classified with the IVD reagent intended purpose**

Standalone software

- Using NGS whole genome data file to provide specific clinical result
- Algorithm to take multiple IVD device outputs and provide specific clinical information
- Imaging software to increase throughput of image analysis for microbiology identification device

➢ **Classified per SW intended purpose**

bsi.

Disclaimer

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

Agenda

Key GSPRs

IVDR General Safety and Performance Requirements most important for software and SaMD.

State-of-the-Art Standards

Important standards that should be considered and applied to demonstrate state-of-the-art and GSRP compliance

Important Guidance

Important standards that should be considered and applied to demonstrate state-of-the-art and GSRP compliance

Lifecycle Models

Waterfall? Agile? Something else?

Questions & Discussion

Key GSPRs for Software

MDR GSPR 14 & IVDR GSPR 13

Construction of devices and interaction with their environment

IVDR GSPR 13.1

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 performances of the devices.* ***Any restrictions on use applying to such combinations shall be indicated on the label and/or in the instructions for use.***

MDR GSPR 14 & IVDR GSPR 13

Construction of devices and interaction with their environment

IVDR GSPR 13.5

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.

IVDR GSPR 13:

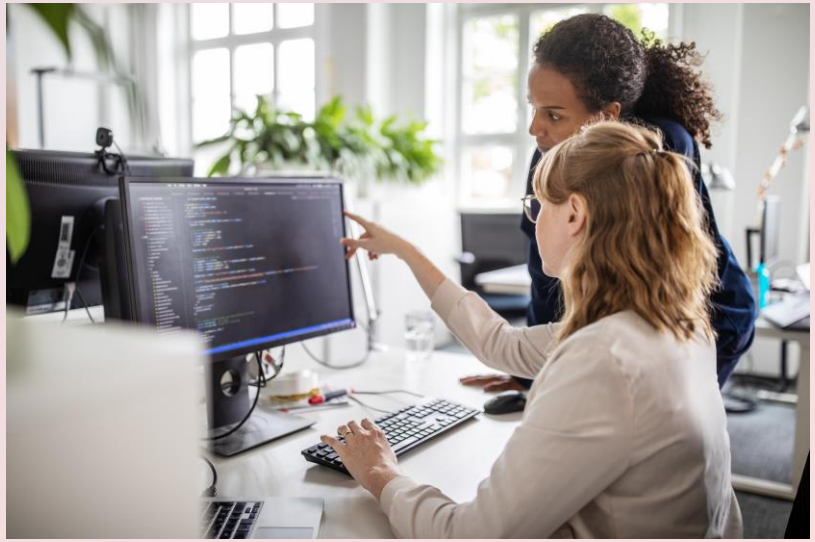
IVDR GSPR 13.1 / 13.5 - Key Points

Software as a Medical Device (SaMD) 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 SaMD clearly defined?
- Are the intended operating systems on which the SaMD executes clearly specified?
- Have designated compatible SaMD/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?



bsi.

IVDR GSPR 13

Construction of devices and interaction with their environment

IVDR GSPR 13.2 (d)

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

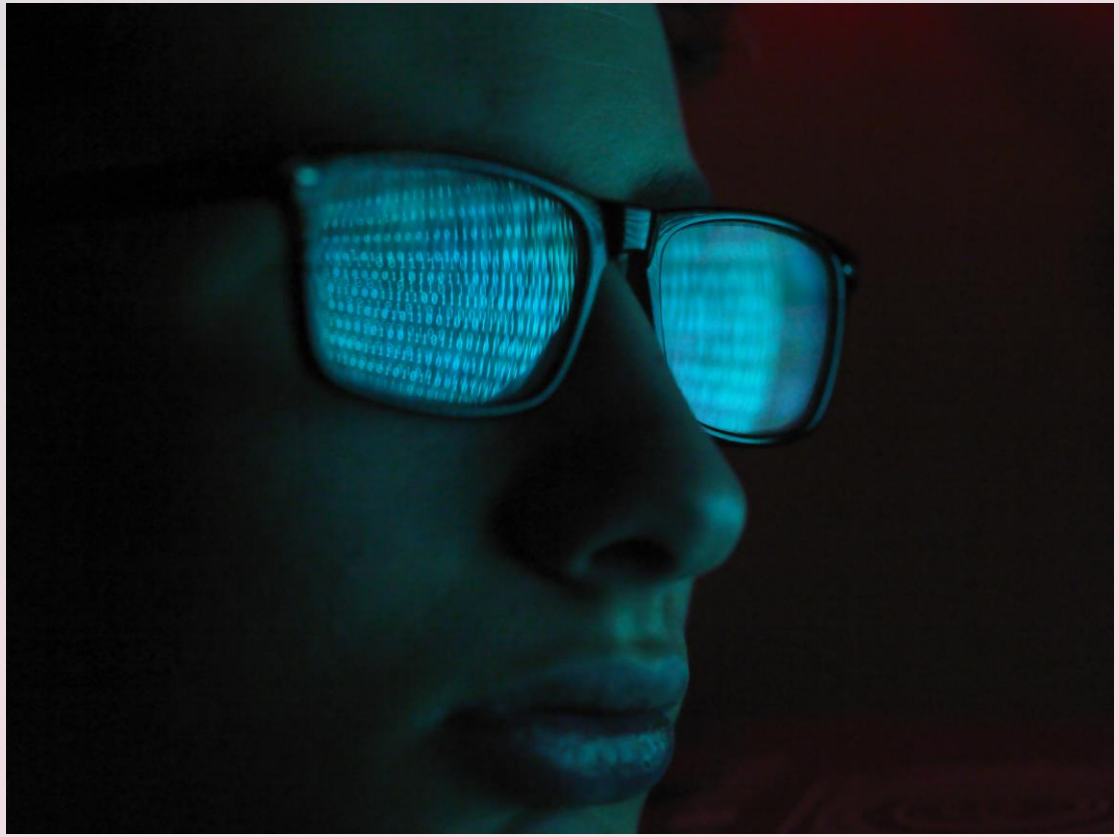
(d) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;

IVDR GSPR 13:

IVDR GSPR 13.2 (d) - Key Points

The Notified Body will want to know:

- What mitigations are in place to harden the SaMD against potential threats from the uncontrolled platform? E.g.:
  - Protections against alteration/removal of the SaMD 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?



bsi.

IVDR GSPR 13 - Construction of devices and interaction with their environment

Construction of devices and interaction with their environment

IVDR GSPR 13.6

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 users, 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.

IVDR GSPR 13:

IVDR GSPR 13.6 - Key Points

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

The Notified Body will want to know:

- What, if any, residual data remains on the mobile device/general purpose computer after the SaMD 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

bsi.

IVDR GSPR 16

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

IVDR GSPR 16.1

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.

bsi.

IVDR GSPR 16

IVDR GSPR 16.1 - Key Points

The Notified Body will want to know:

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

bsi.

IVDR GSPR 16

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

IVDR GSPR 16.2

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.

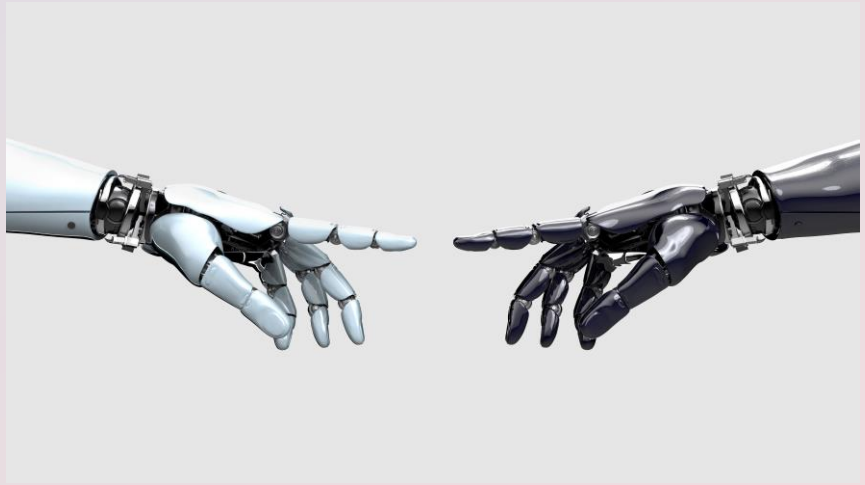
bsi.

IVDR GSPR 16

IVDR GSPR 16.2 - Key Points

The Notified Body will want to know:

- 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) / Performance Evaluation (IVDR) of Medical Device Software



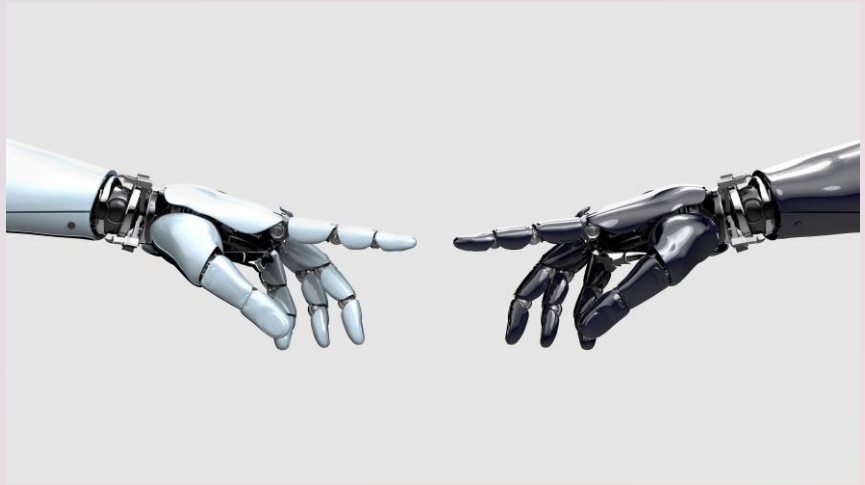
bsi.

IVDR GSPR 16

IVDR GSPR 16.2 - Key Points (cont'd)

The Notified Body will want to know:

- Which standards and associated versions have been applied?
- Which guidance documents and associated versions have been applied?
  - MDCG Guidances
  - IMDRF Guidances
  - MEDDEV Guidances
  - FDA Guidances
- If a harmonized standard has been published in the Official Journal of the European Union (OJ), has it been applied? (e.g. EN 14971:2019 / EN 14971:2019+A11:2021).
- Why are the set of standards and guidances and versions applied considered representative of state-of-the-art?



IVDR GSPR 16

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

IVDR GSPR 16.3

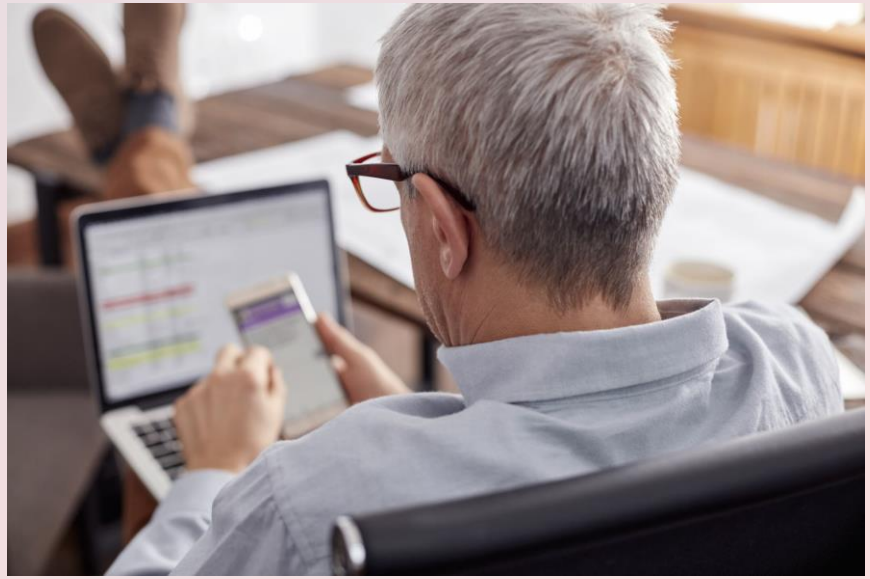
Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use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

IVDR GSPR 16

IVDR GSPR 16.3 - Key Points (cont'd)

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?



bsi.

IVDR GSPR 16

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

IVDR GSPR 16.4

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

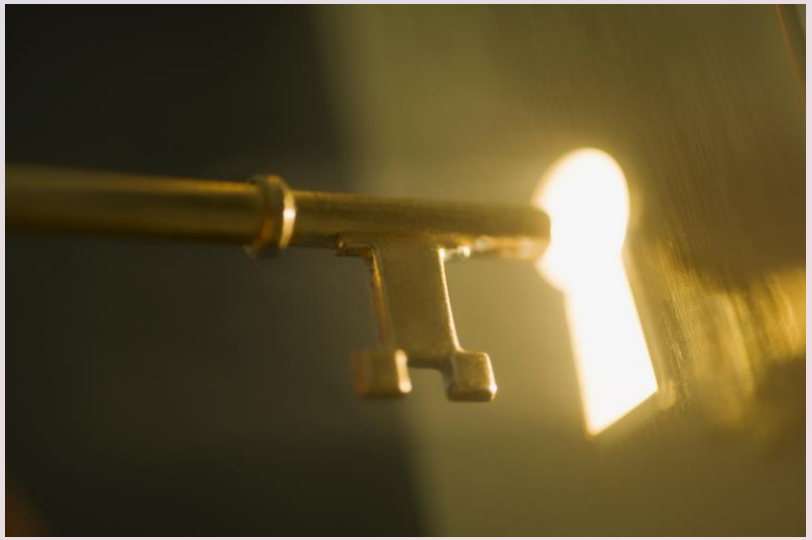
bsi.

IVDR GSPR 16

IVDR GSPR 16.4 - Key Points (cont'd)

The Notified Body will want to know:

- Are security mitigations clearly specified in requirements documents?
- Are steps needed to configure and connect the SaMD 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?

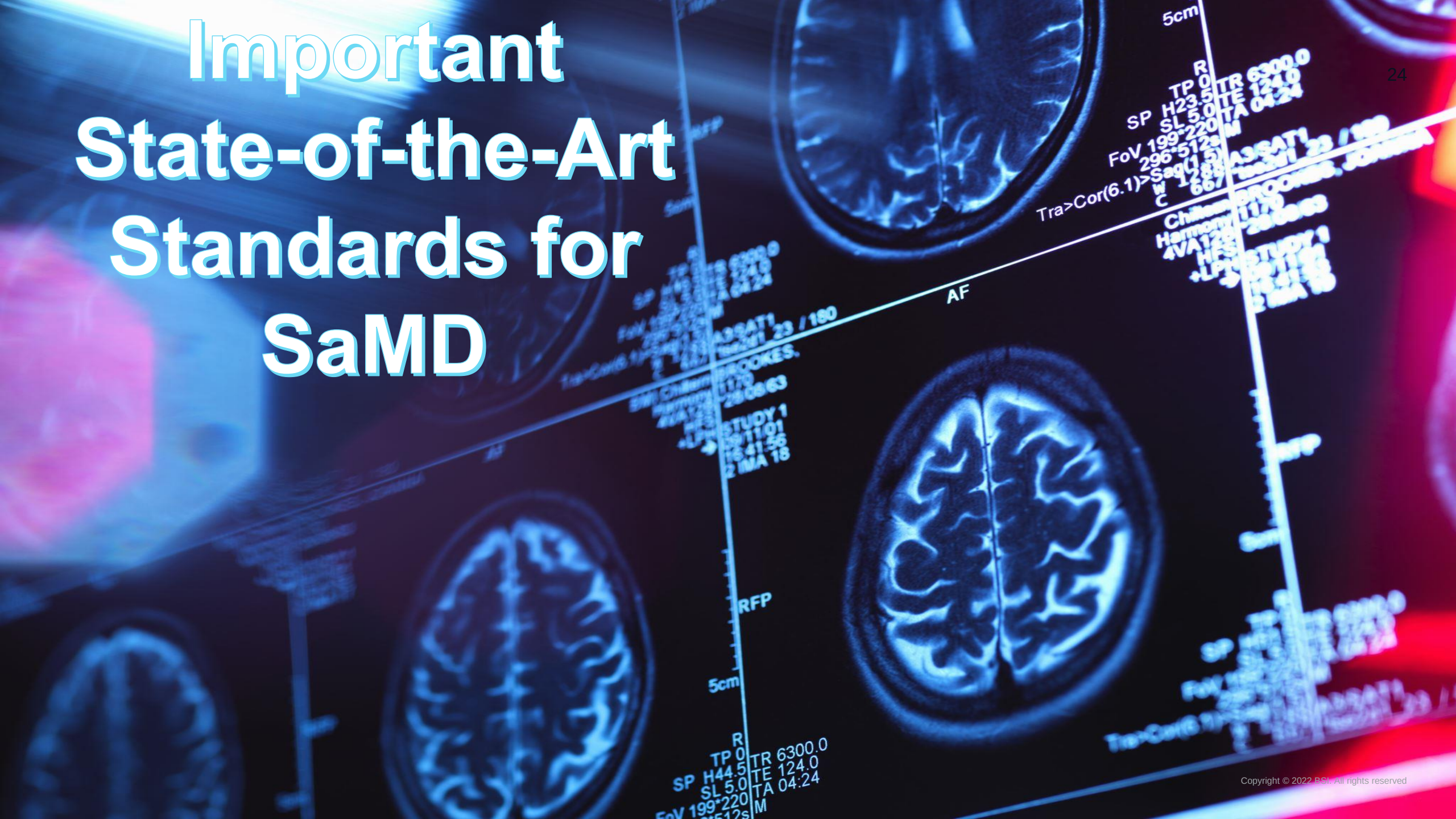


NOTE: Even if the SaMD is not designed to connect to a network or to the internet, GSPR 16.4 (IVDR) still applies.

Many other GSPRs may apply for a particular SaMD based on its **Intended Purpose**.

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

Important State-of-the-Art Standards for SaMD



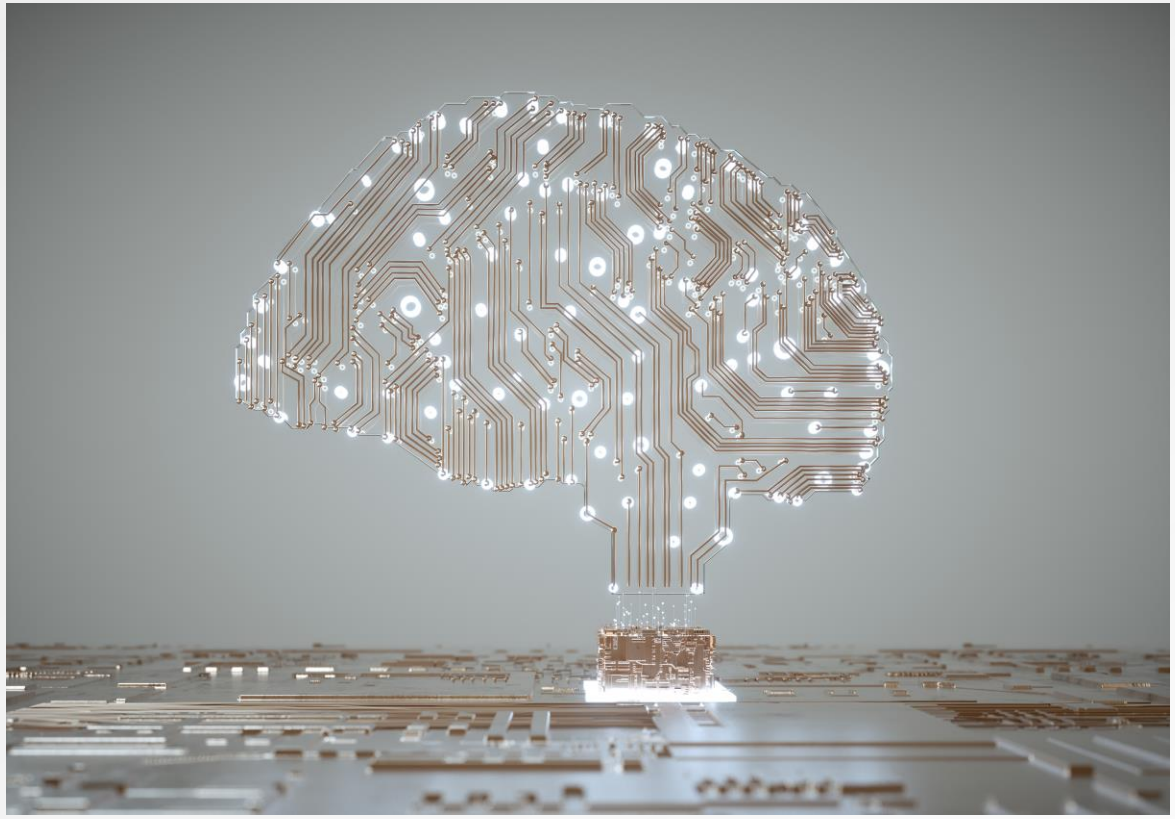
EN 62304:2006+A1:2015

Current SOTA for all MDSW (SaMD and SiMD)

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**



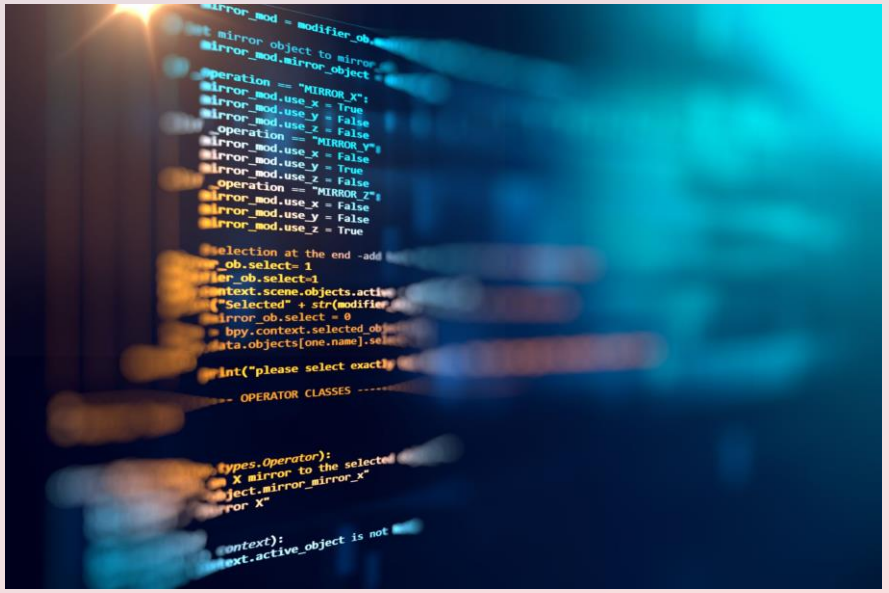
MEDICAL DEVICE SOFTWARE
SOFTWARE SYSTEM that has been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed or that is intended for use as a medical device.

EN 62304:2006+A1:2015

Key Points

The Notified Body will want to know:

- Is an **EN 62304 Compliance Matrix** provided?
- Is SW Safety Classification correct? ➔ Start with [C], lower based on:
  - Only mitigations external to the software; or
  - Severity of harm of SW failure is lower than SERIOUS INJURY/Death
- 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
- SW risk assessment provided (or included in system risk documents)?
- All known anomalies documented [A, B, C]? ➔ Each anomaly assessed for risk and justified [B, C]?



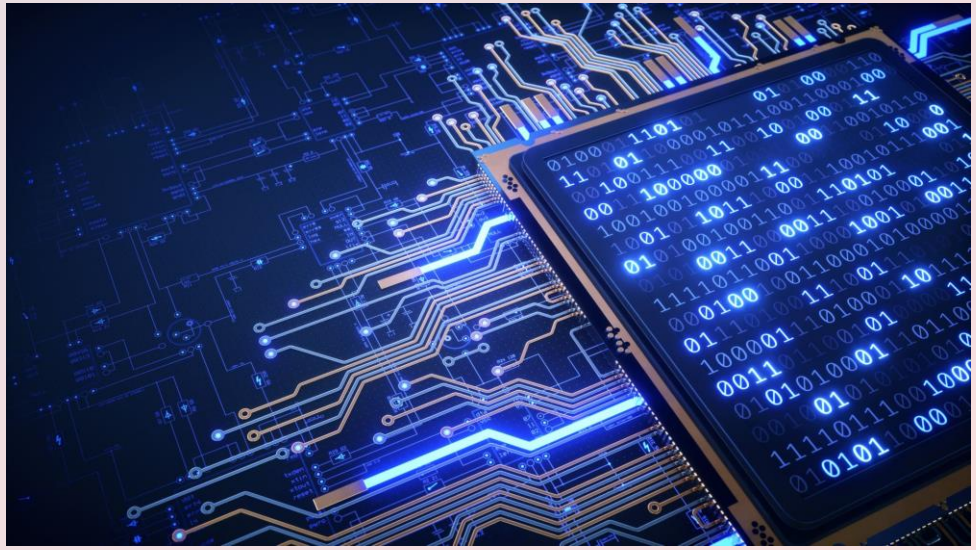
bsi.

EN 62304:2006+A1:2015

Key Points

Common Issues:

- Missing EN 62304 matrix or not sufficiently detailed (doc & section/page references)
- Incorrect SW Safety Classification
- Incomplete/Missing SW Development Plan
- Missing/incomplete Unit Verification [B, C] ➔ “White Box” testing ➔ Not the same as SW System Testing (“Black Box”)
- Missing/incomplete SW Integration testing [B, C]➔ “White Box”/ “Grey Box” ➔ Not the same as “System Integration” ➔ Focus is on integration of SW Items
  - Can be combined with SW System Testing, but this needs to be clearly documented (e.g. in SW Development/Testing Plans)
- Known anomalies list not provided
- Known anomalies not risk assessed and justified [B, C]
- Procedure and environment used to create the software not provided or not sufficiently detailed



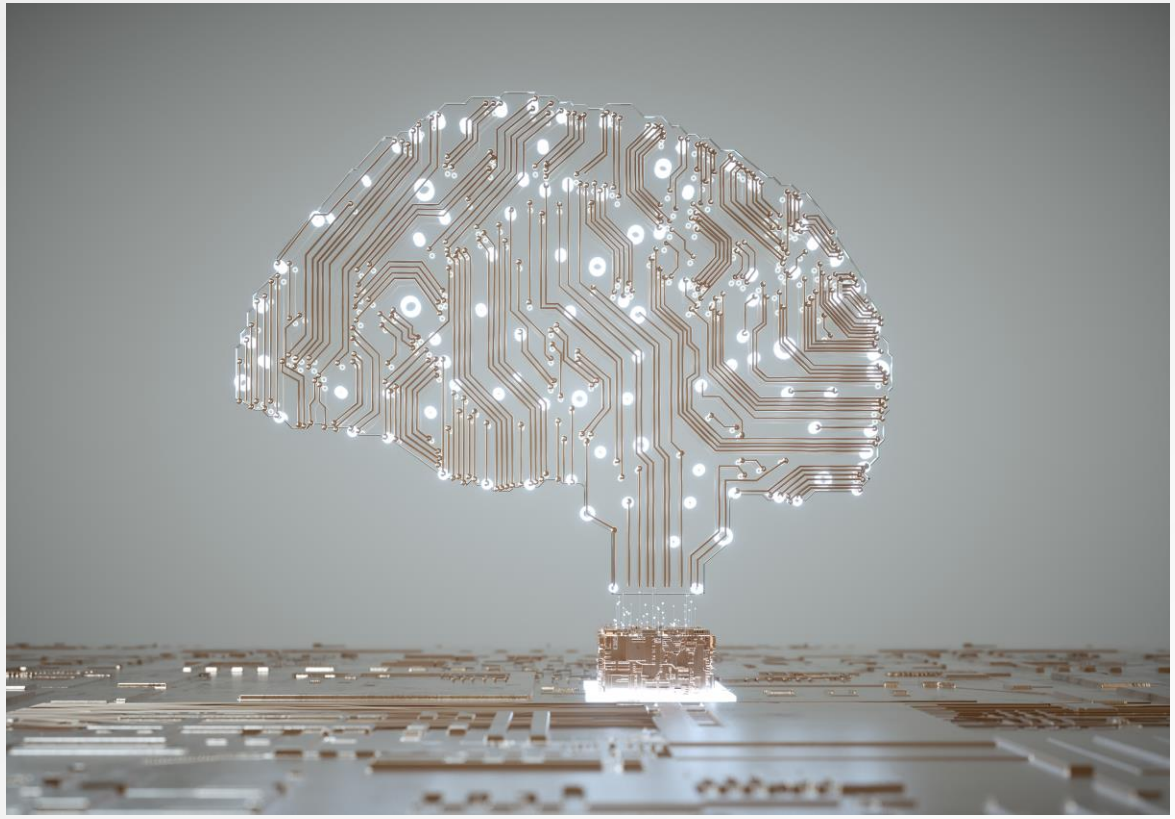
EN 82304-1:2017

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

Key Points

The Notified Body will want to know:

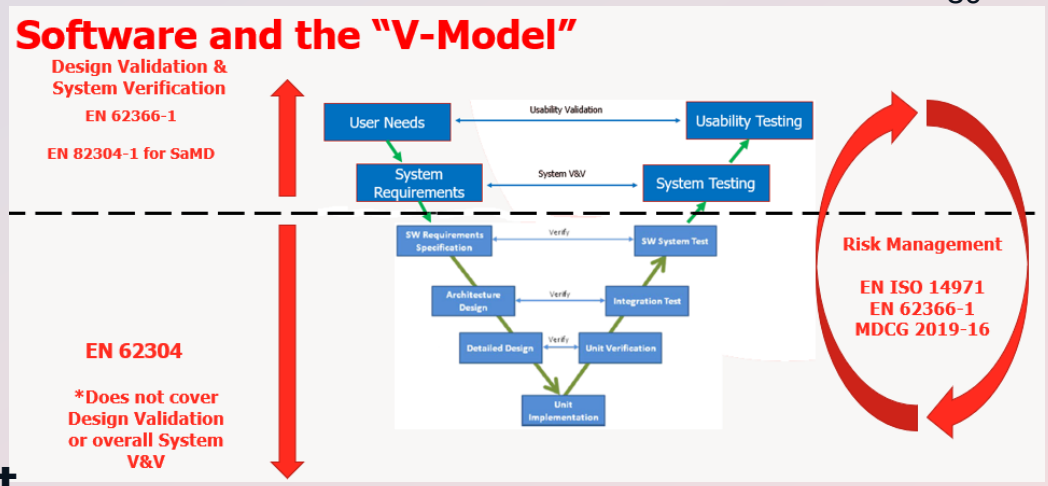
- Has **EN 82304-1 been applied** for SaMD? ➔ Is an **EN 82304-1 Compliance Matrix** provided?
- Is there a documented intended use including user profile and operational environment?
- SW product requirements established? E.g. characteristics related to safety and security; risk control measures; configuration; interfaces to other products
- System requirements established? E.g. functionality, localization, user interface, SW and HW platforms, detection of security compromise, protection of essential functions
- Verification of system requirements performed and documented?
- SW lifecycle process aligned with EN 62304?
- Has Software Product Validation been conducted? Is it appropriate (see next slide)

EN 82304-1:2017

Key Points (cont'd)

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 82304-1:2017

Key Points

The Notified Body will want to know:

- Are required contents present in Instructions for Use? E.g. Operation information, installation instructions, decommissioning and disposal, … many others!
- Are required contents present in the Technical Description? E.g. System requirements, Supported SW platforms, maintenance requirements, technical security options, … many others!
- Required additional information if intended for an IT network outside of manufacturer control? E.g. Characteristics and configuration of IT network, Specifications of the IT network including security and protection against malware/malicious software, Hazardous situations from failure of the IT network … many others!
- Required post-market activities provided for?
  - Validation includes decommissioning and disposal by end users?
  - Software Maintenance: Modification ➔ Revalidation ➔ Users Informed

bsi.

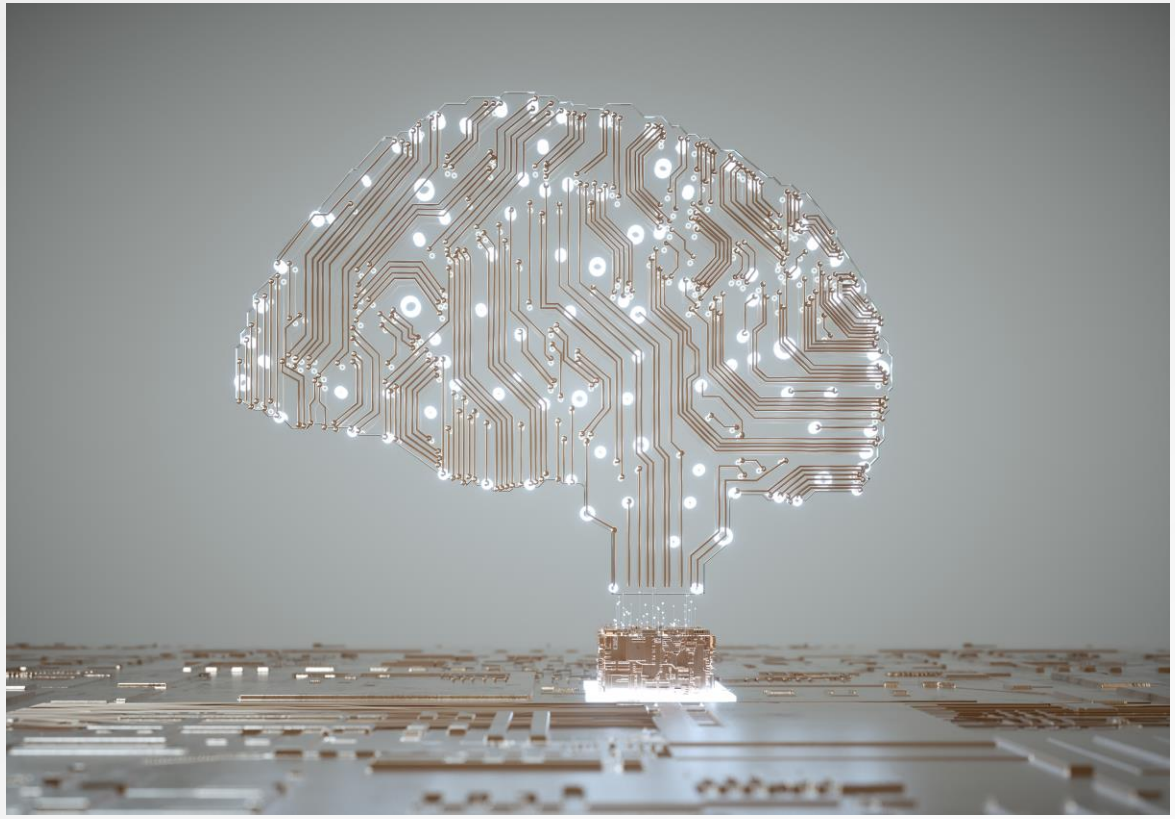
EN 62366-1:2015+A1:2020

Current SOTA for usability engineering for medical devices

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

Areas covered:

- **Principles (General requirements, usability engineering file, etc.)**
- **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 (UIOP)



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

EN 62366-1:2015+A1:2020

Key Points

The Notified Body will want to know:

- Has **EN 62366-1 been applied** for SaMD?
  ➔ Usability process constitutes part of the design validation
- 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? (e.g. based on risk, PMS data, etc.)
- 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?

bsi.

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

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

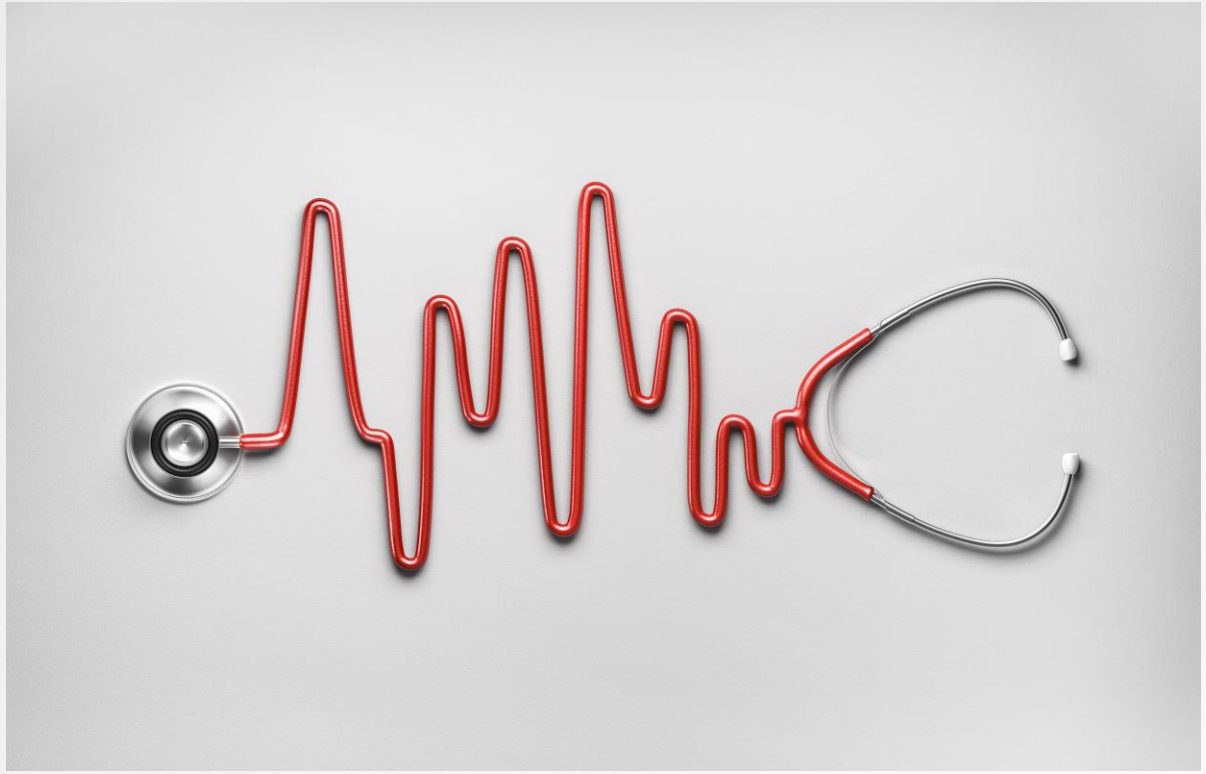
Important Guidance for SaMD

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**
- **Decision steps for classification of MDSW under IVDR**
- **Considerations for placing MDSW on the market and conformity assessment:**
  - As a medical device in its own right ➔ SaMD
  - As an integral component/part of a device ➔ SiMD
- **Consideration of changes to MDSW**
- **Examples (MDSW and non-MDSW)**
- **Application of IMDRF risk classification for MDR Rule 11**



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

Key Points

The Notified Body will want to know:

- Are MDSW / non-MDSW modules properly classified? Non-MDSW examples (no clinical function; no impact to risk/security):
  - Invoicing and other accounting functions
  - Providing a link to the social security system for reimbursement
  - SW only for: storage, archival, communication* or simple search

  *If the communication SW module could be interrupted/altered/intercepted in a way that would lead to a safety/security risk, it should be considered part of the MDSW (e.g. may be SOUP as per EN 62304 definition)
- 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

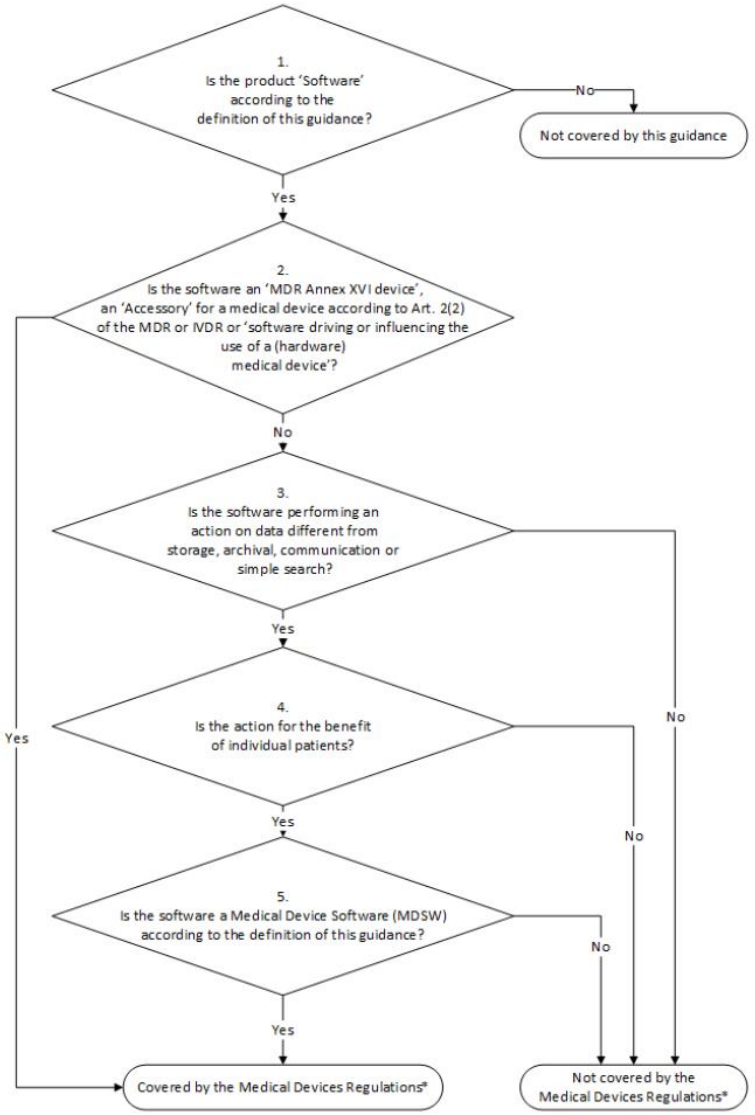


Figure 1 – Decision steps to assist qualification of MDSW

Medical Devices Regulations* refers to the two applicable regulations: Regulation (EU) 2017/745 on Medical Devices (MDR) and Regulation (EU) 2017/746 on *In Vitro* Diagnostic Medical Devices (IVDR)

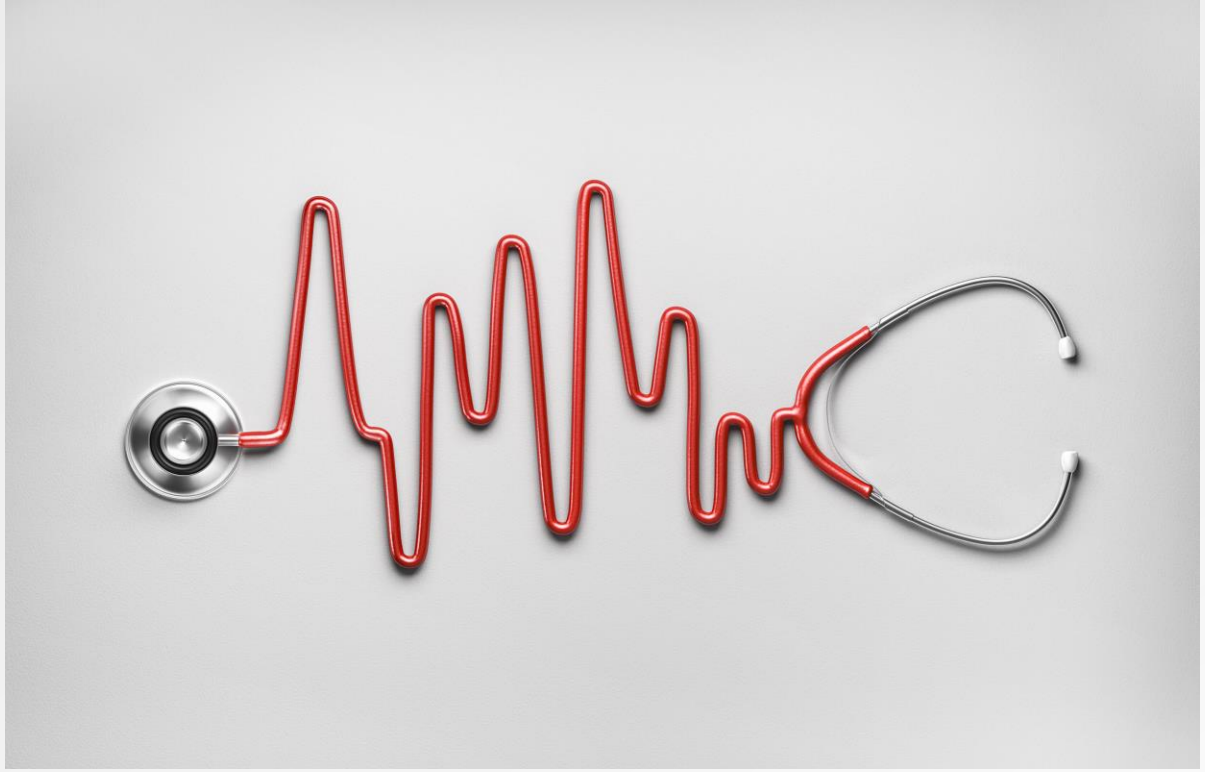
MDCG 2021-24

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**



MDCG 2021-24

Key Points

- *"Software is also an active device[13]. **Software should be reviewed <u>not only</u> in the context of Rule 11[15]."***

[13] MDR Annex VIII 2.7
[15] MDCG 2019-11

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 health data including basal body temperature (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).

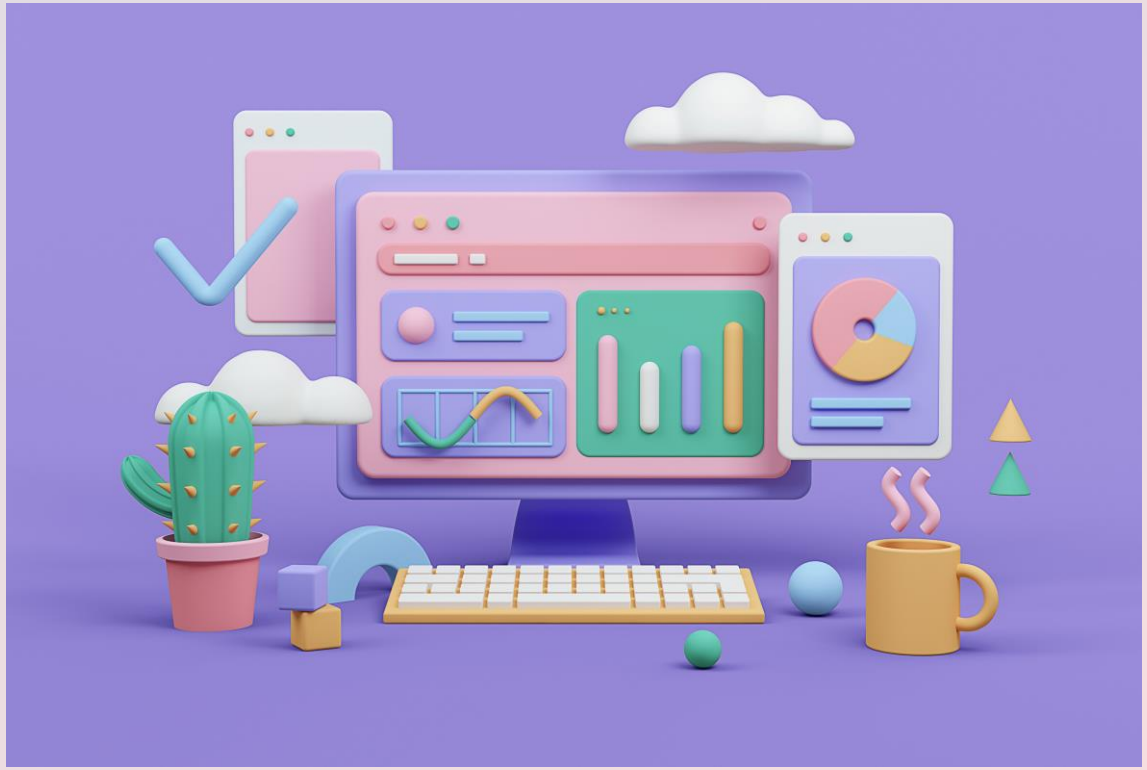
MDR Rule 11 Examples

MDCG 2021-24

Key Points

- **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**



bsi.

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 Survellance and Vigilance
- Other Legislation and guidance

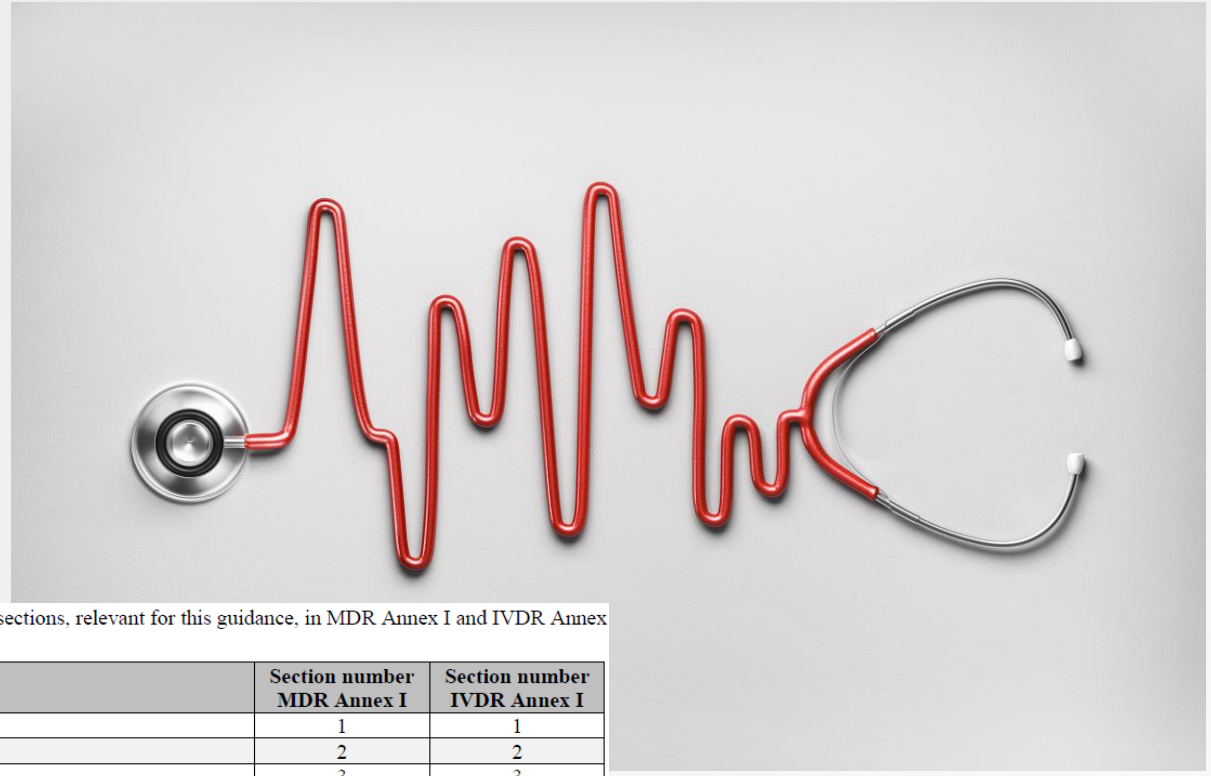


Table 1: Correspondence table between sections, relevant for this guidance, in MDR Annex I and IVDR Annex I

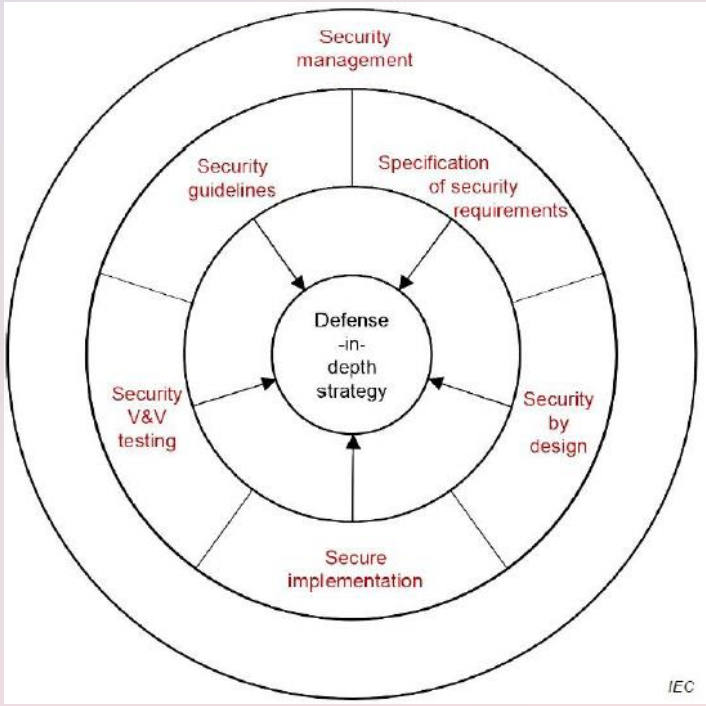
Main topic	Section number MDR Annex I	Section number IVDR Annex I
Device performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
Combination/connection of devices/systems	14.1	13.1
Interaction between 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:

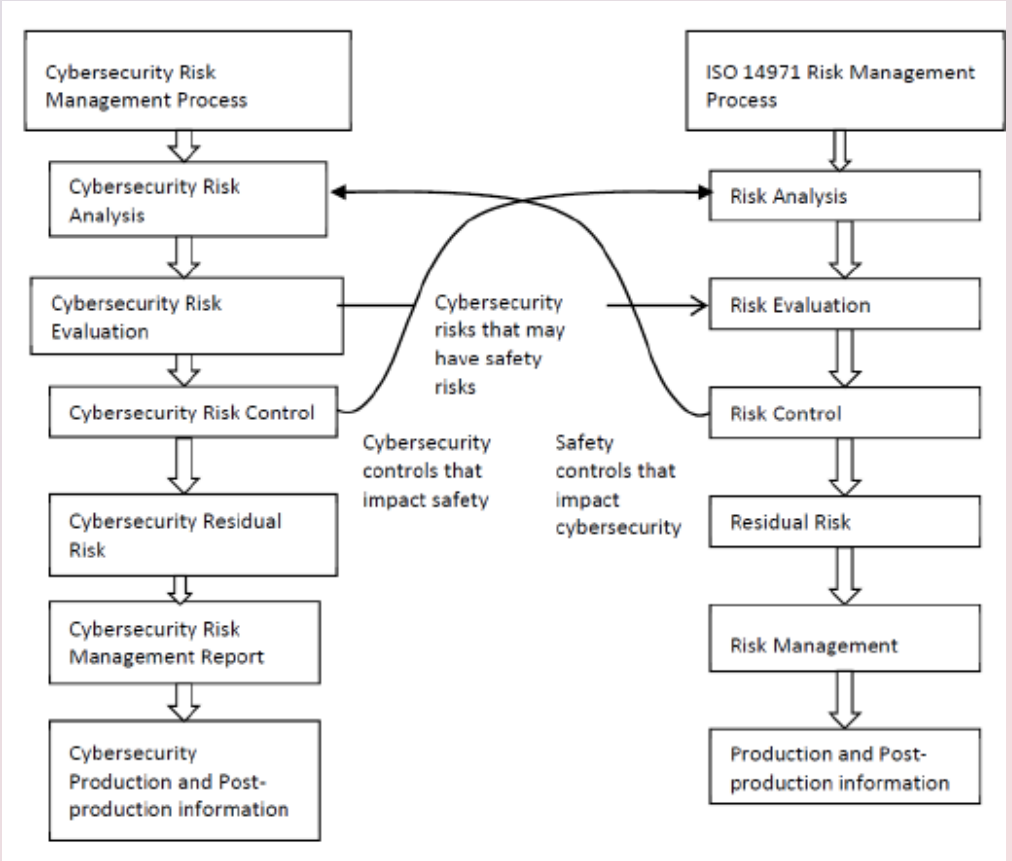
- Is security integrated with the development and risk management processes? ➔ **Should not be "bolted on" at the end!**
- Is there a security risk management plan?
- Is there a security risk assessment? ➔ Should minimally consider threats to Confidentiality, Availability, Integrity
- Has security-focused 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?

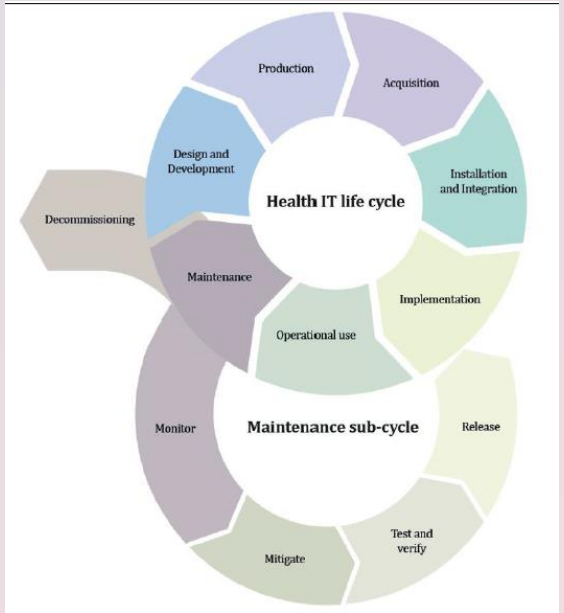


MDCG 2019-16

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.)



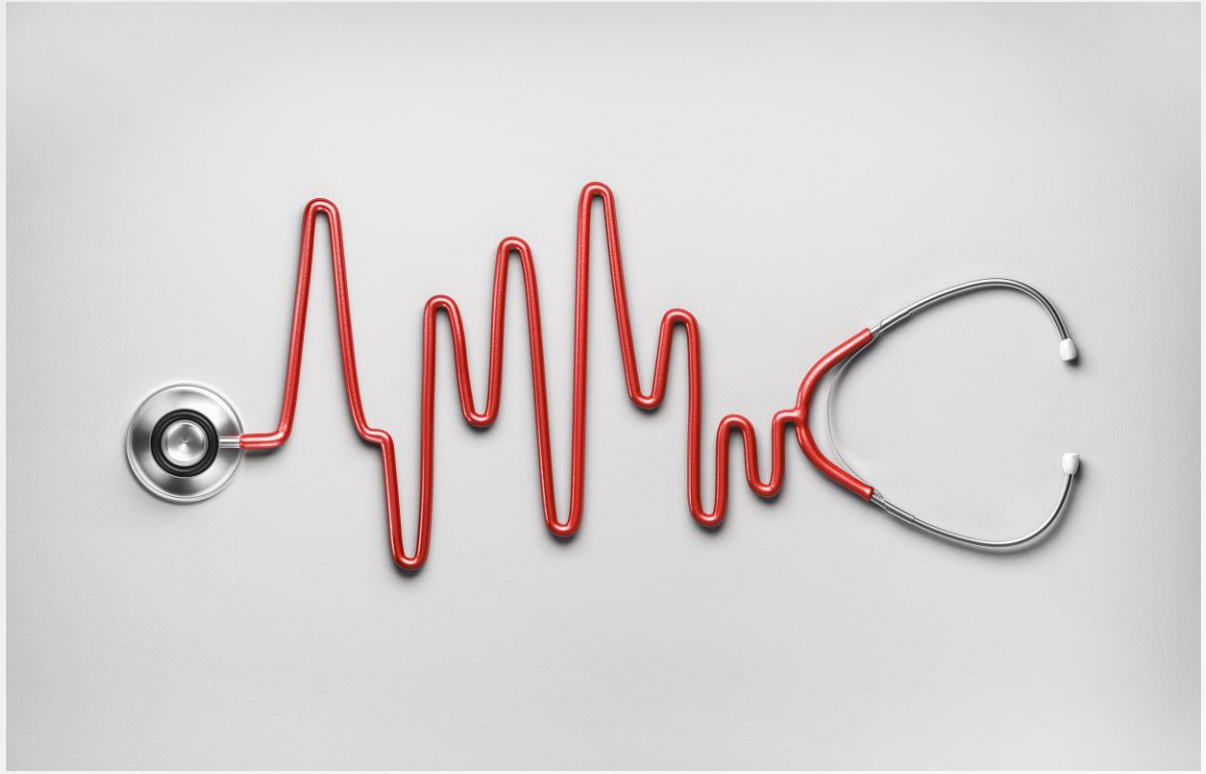


MDCG 2020-1

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)

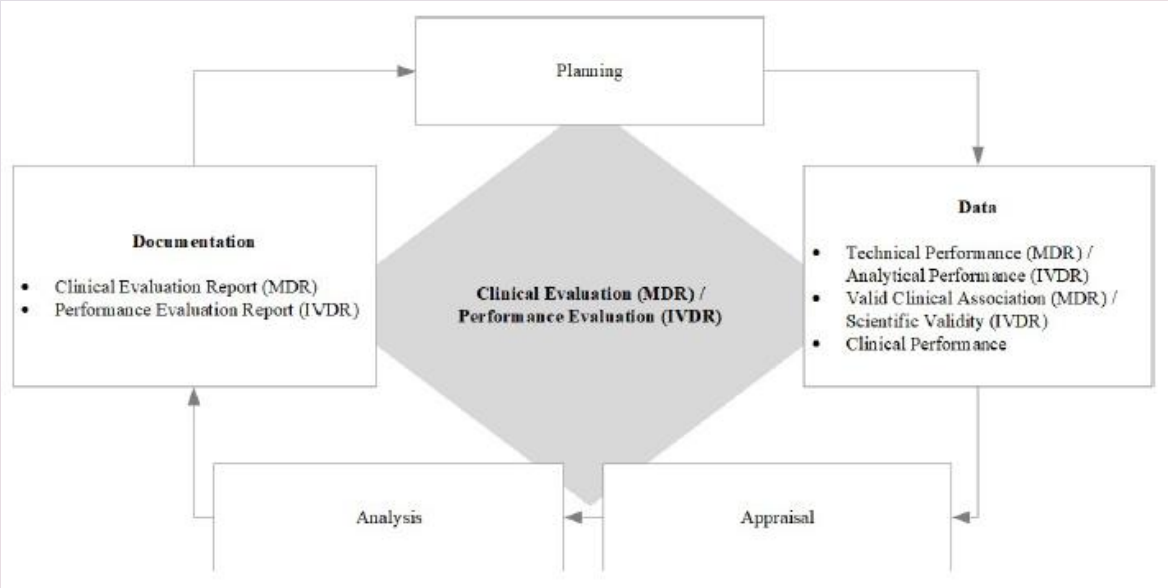
An assessment and analysis of data to establish or verify the SCIENTIFIC VALIDITY, the ANALYTICAL and, where applicable, the CLINICAL PERFORMANCE of a device.

MDCG 20201-

Key Points

The Notified Body will want to know:

- What clinical investigations / performance studies have been conducted to support the claims made for the SaMD?
- Where equivalence is claimed, is the equivalence analysis appropriate?
  - Clinical equivalence (Same)
  - Technical equivalence (Similar)
  - Biological equivalence (Same)
  - Manufacture has access to full technical file of claimed equivalent device
- Is state-of-the-art appropriately considered and documented in the CER / PER?
  - Should consider other available treatments / diagnostic solutions (not just similar devices)



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

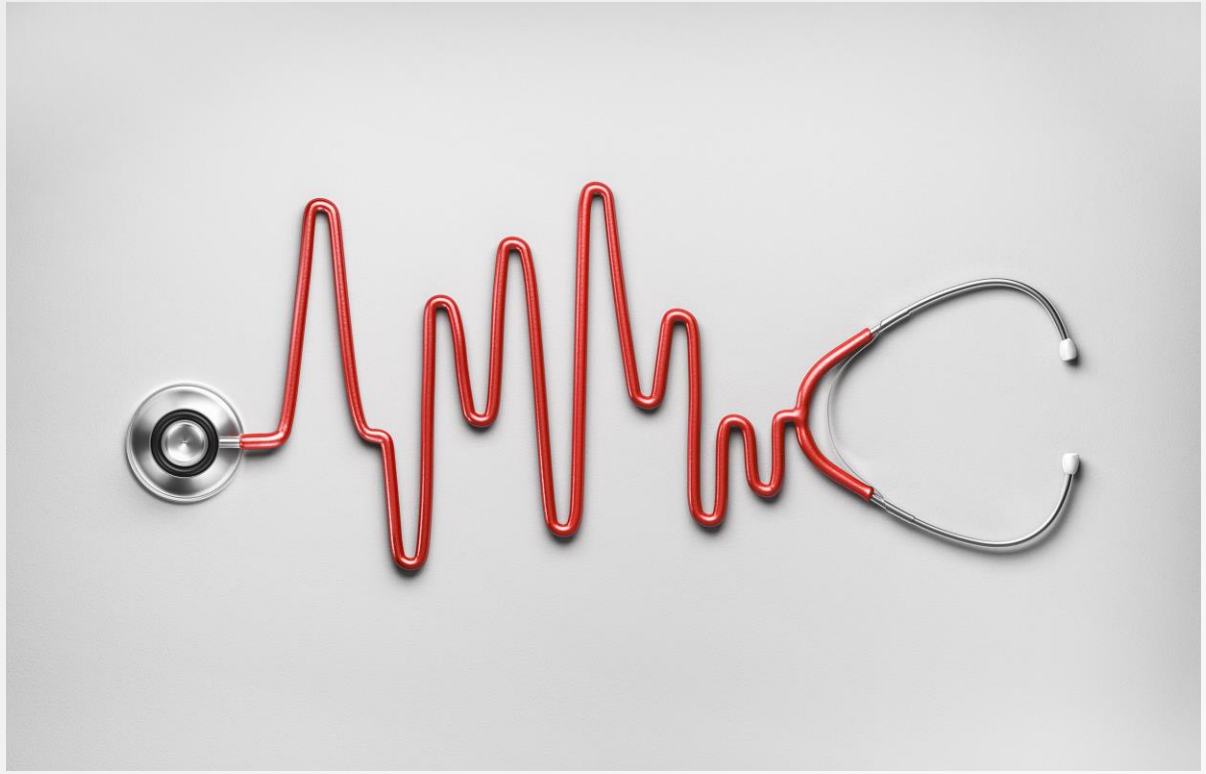
(see also MEDDEV 2.7/1 Rev. 4)

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

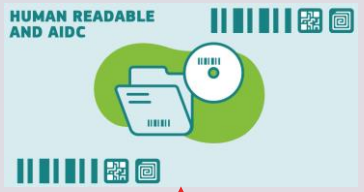
The Notified Body will want to know:

- 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:

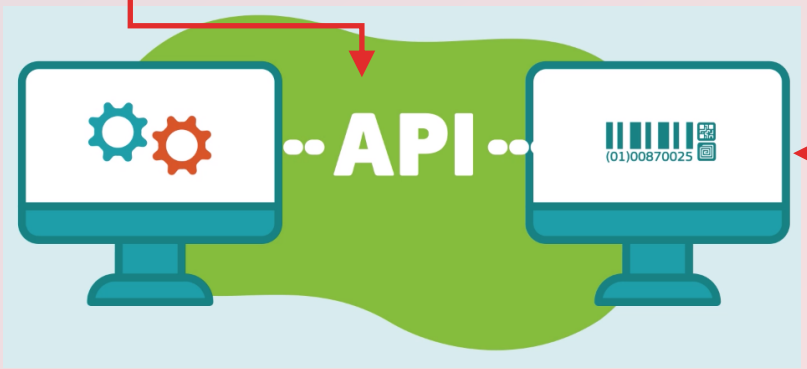
a) each packaging level shall bear the human readable and AIDC representation of the complete UDI. The UDI that is applied to the physical medium containing the software and its packaging shall be identical to the UDI assigned to the system level software;

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.



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 come**…

Development Lifecycles

Agile vs. Waterfall vs. Something Else?

- BSI is seeing more SW submissions developed according to an Agile methodology
- “Agile Manifesto” needs to accommodate regulatory requirements
- Following an “Agile” process in the contect of regulated SW development requires robust tools and processes:
  - Requirements management/Test Management/Traceability
  - Configuration Management
  - Change Management
  - Test Automation

How to rapidly ascend the “spiral staircase” without falling down the stairs?

Agile Manifesto - Regulatory accommodations - Processes

https://agilemanifesto.org/

NBs want to see well-defined **processes:**

- Product Development
- **Software Development**
- **Software Maintenance**
- Risk Management/**SW Risk Management**
- **SW Configuration Management**
- **SW Problem Resolution**
- Usability
- Post-market surveillance
- Cybersecurity risk management
- Clinical evaluation
- …and many more!

NOTE: Processes described by EN 62304 shown in bold above.

bsi.

Agile Manifesto - Regulatory accommodations - Documentation

https://agilemanifesto.org/

NBs review **documentation**, including:

- User needs
- System requirements
- Product requirements
- **Software (or firmware) Requirements specifications**
- **Software architecture design**
- **Software detailed design**
- **Software unit verification results**
- **Software integration plans and reports**
- **Software system test protocols and reports**
- Risk assessments/**SW risk assessments**
- **Software release documents**
- **List of known anomalies**
- Product/sub-system verification protocols and reports
- System verification protocols & reports
- Design validation protocols & reports
- Usability protocols & reports
- And many more…!

NOTE: Outputs/deliverables required by EN 62304 shown in bold above.

Agile Manifesto - Regulatory accommodations - Planning

https://agilemanifesto.org/

NBs review many **plans**:

- System design V&V plan(s)
- Risk management plan
- Clinical evaluation plan
- **Software development plan:**
  - **SW development standards, methods and tools planning**
  - **Software integration and integration testing planning**
  - **Software VERIFICATION planning**
  - **Software RISK MANAGEMENT planning**
  - **Documentation planning**
  - **Software configuration management planning**
- **Software maintenance plan**
- Post-market surveillance plan
- PMCF plan
- Cybersecurity monitoring plan
- And many more…!

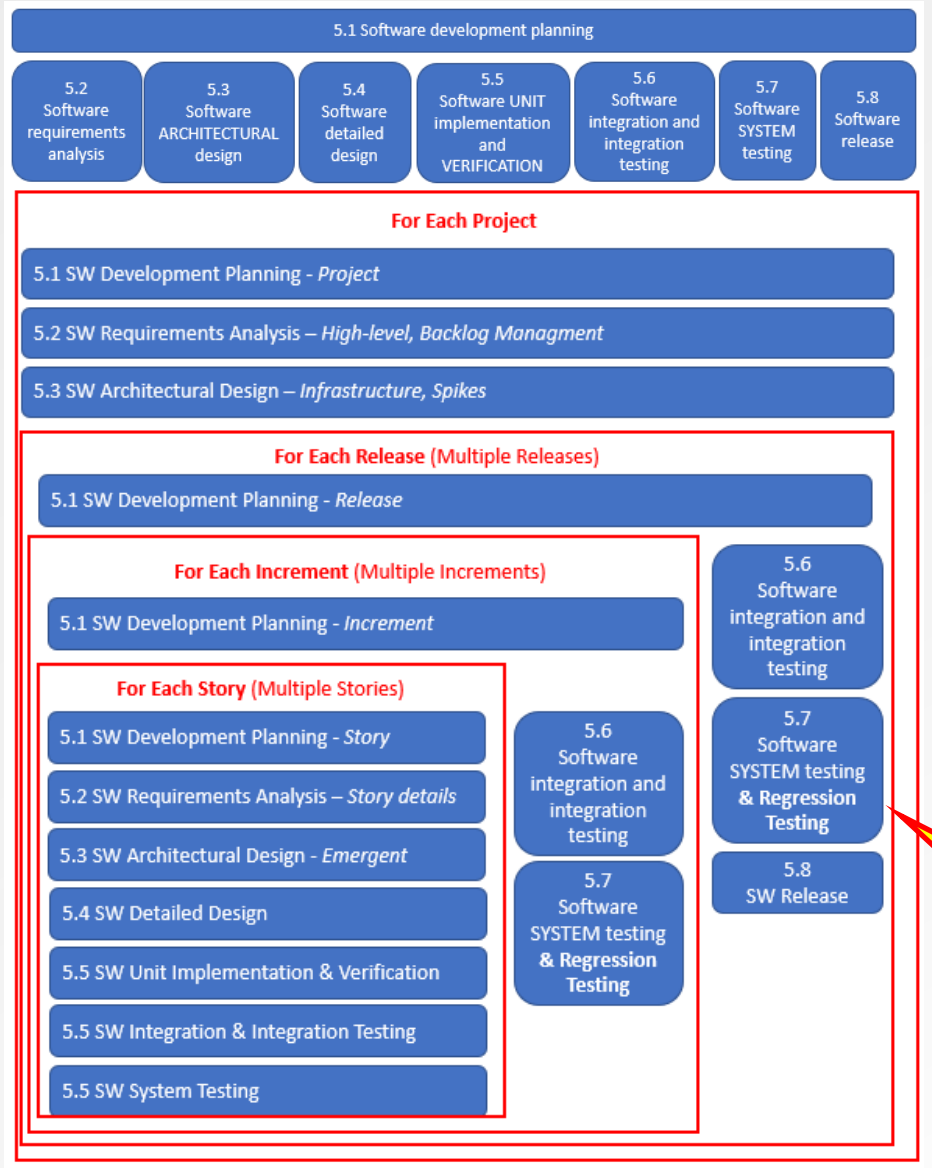
NOTE: Planning activities required by EN 62304 are shown in bold above.

Mapping 62304 activities to an incremental SW development model – AAMI TIR45: 2012/(R)2018

AAMI TIR45: 2012/(R)2018 - *Guidance on the use of AGILE practices in the development of medical device software*. ➔ Explains how to apply agile concepts while remaining compliant with EN 62304.

Conceptually, **perform each required SW activity for each incremental SW release**.

Care is needed for subsequent release "Regression Testing" to ensure **newly added features or fixed bugs** from the product backlog did not introduce new bugs.



Required EN 62304 activities

SW requirements and architecture grow/evolve across all iterative releases until final release

Required EN 62304 activities ***performed iteratively***

Regression Testing performed for each iteration ➔ Higher demand for testing ➔ One solution is ***automated testing***

Adapted from AAMI TIR45 Figure 4

Best Practices for Notified Body Software Submissions

Summarize results of all software V&V testing in the STED

If the submission relates to SW changes/bugfixes to an approved product, clearly **describe the SW changes in the STED**

Provide a **SW revision history** ➔ Indicate **approved versions** and well as **formally tested versions**

Provide a **Document Index** in the STED ➔ Help NBs help you

Test Report	Document/Version (Ref. No.)	Test Summary	SW version(s) tested
Software Systems Test Report	12345 Ver. A (Ref. 01)	X of Y tests executed, Z tests passed, W failed	a.b.c.d
SW Integration Test Report			
SW Unit Test Report			
Code Review Report			
Static Analysis Report			

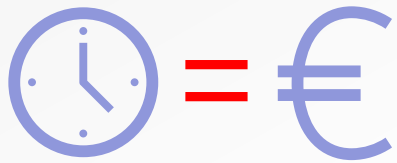
Example

Change ID	Change Type	Summary Description	Risk & Severity	Affected Version	Implemented in Version
1234	Bug	The software crashed when the 'Interrogate' button is pressed	R='Low'; S='2'	a.b.c.d	a.b.c.e
5678	Enhancement	Change button color from grey to blue	R='None'; S='0'	a.b.c.d	a.b.c.f

Example

Version	Comments	Date
a.b.c.d	**Initially CE Marked version**	**2019-01-01**
a.b.c.e	SW Integration Test Suite 1	
a.b.c.f	SW Integration Test Suite 2	**2020-08-01**
a.b.c	**SW System Test & Final Release for this submission**	**2020-12-31**

Example



Best Practices for Notified Body Software Submissions – Expected SW documents - Tracing

NBs conduct **detailed V&V and risk audits** (sampling), so…

- **Trace matrices** should be provided (e.g. SW requirements to SW test cases)
- **Risk management** documents should allow **traceability** from **mitigations➔requirements** and from **requirements➔V&V** tests
- Technical auditors need to understand **how the test operates➔** If automated tests are used, **plain-language summaries** of the test sequence and acceptance criteria are helpful (but provide the test script code too)
- **Raw data** must be observed as part of the detailed audits
  Manual tests: Provide **test datasheets**
  Automated tests: Provide **execution/log files**

User Needs and Validation			Design Inputs, Risk and Verification			
ID	User Need	Validation Tests	ID	Design Input	Risk ID	Verification Tests
UN0001	Display	VAL0001	SPR0019	Liquid ingress protection	N/A	VER0006
			SPR0073	Touch screen Protection 2	N/A	NONE
UN0002	Device remote control	VAL000	SPR0015	Remote interface	N/A	VER0008
			SPR0016	mote Cable gth	N/A	VER0006
			SPR00	Single push button	RISK0010	VER0005
			SPR0018	Biocompatibility	N/A	VER0006
			SPR0019	Liquid ingress protection	N/A	VER0006
			SPR0020	Audible feedback	N/A	VER0009
				Overdose		

Example

bsi.

Time for your IVDR application is now

Questions?

We are accepting applications for IVDR certification

BSI has capacity across the full scope of our IVDR designation and we are accepting IVDR applications.

Request a quote

https://www.bsigroup.com/en-GB/medical-devices/forms/contact-us-med-dev/

Contact us

Email: medicaldevices@bsigroup.com