Regulatory developments in cybersecurity of medical devices under Regulation (EU) 2017/745 and Regulation (EU) 2017/746

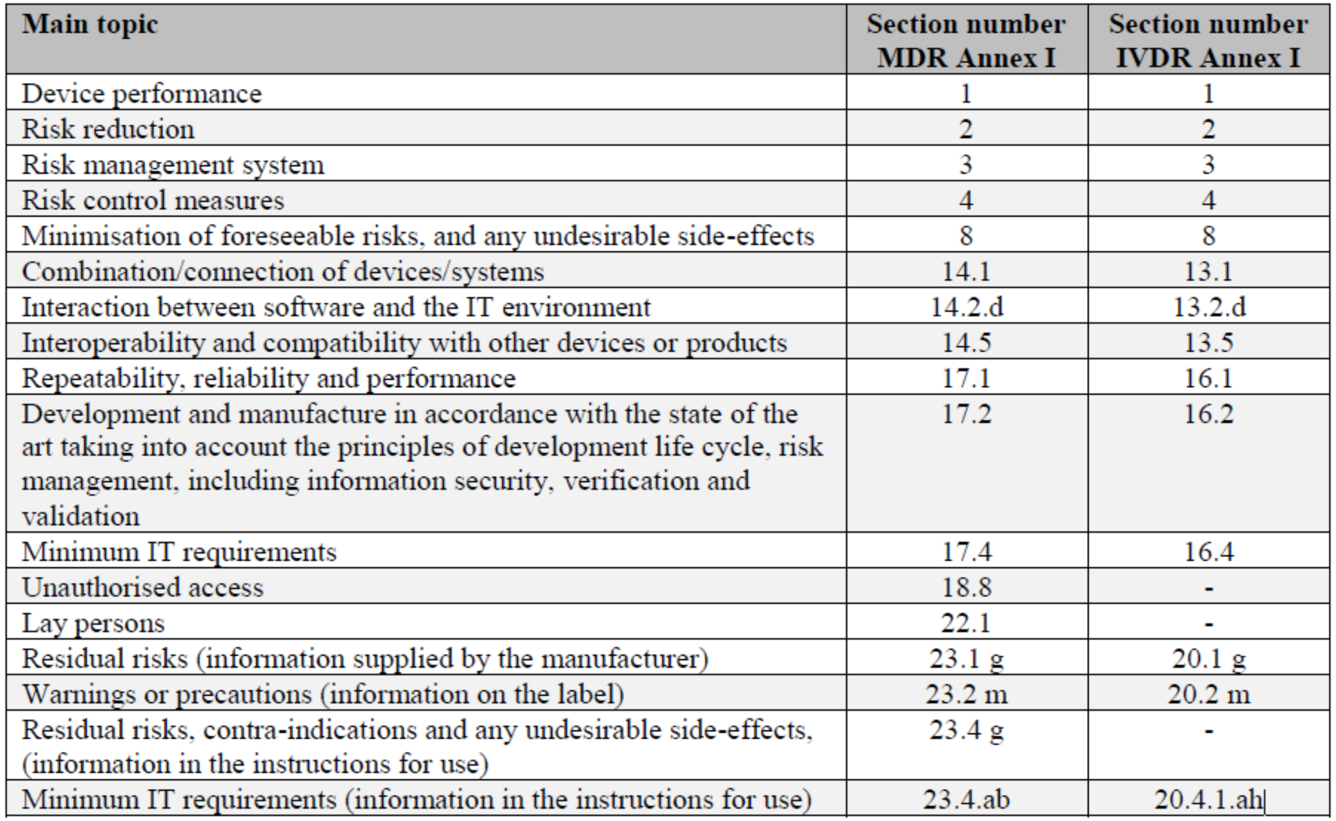
Directorate-General for Health and Food Safety (DG SANTE)
Medical Devices and HTA unit
Nada Alkhayat

Health

New Regulations - MDR (2021) and IVDR (2022)

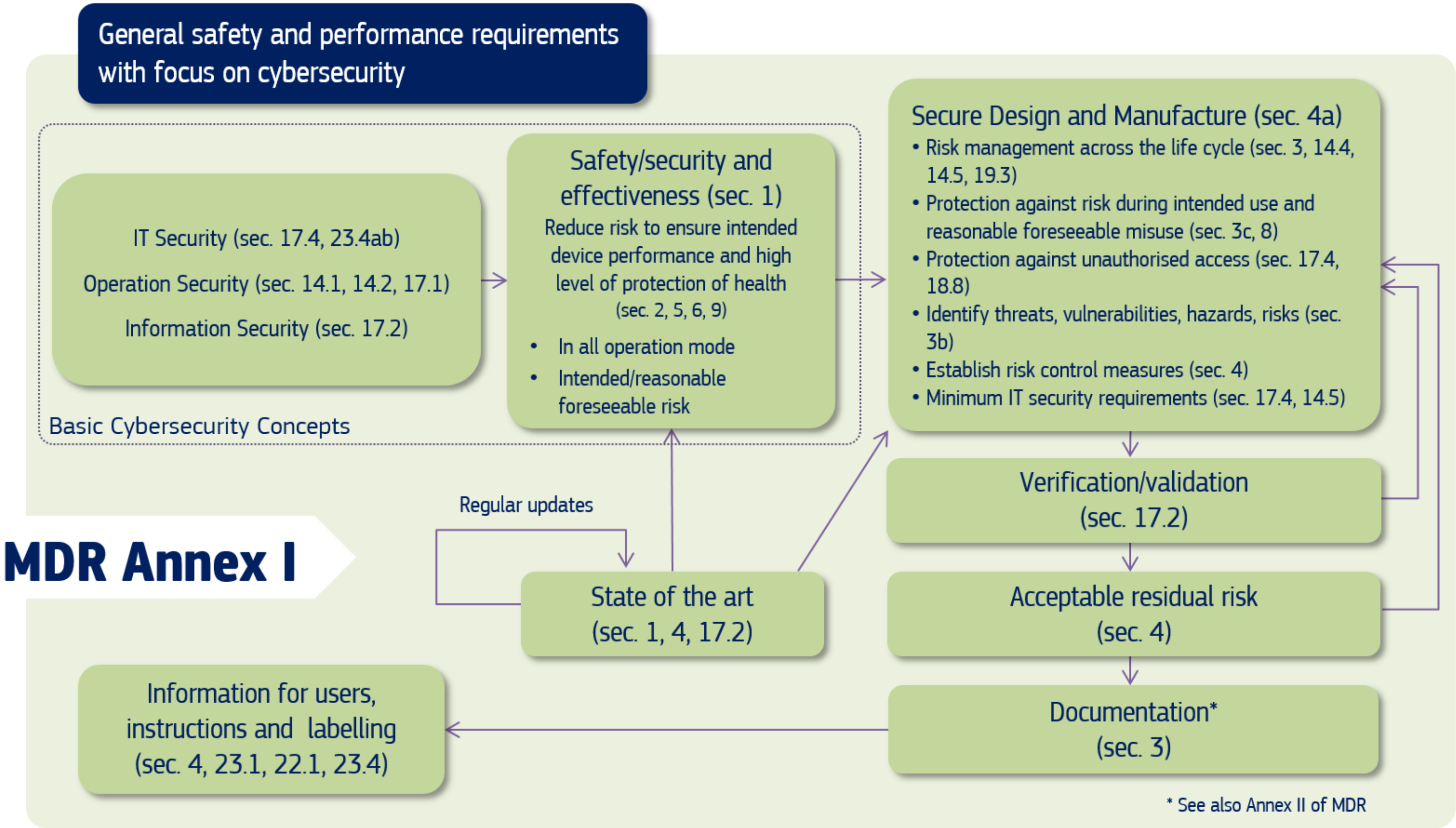
- New regulations bring about an increased expectations for all types of medical devices including those incorporating software and independent Medical Device Software (MDSW)
- New classification rules specific to software
- Increased PMS and Vigilance
- Risk Management
- Re-inforcement of the ’lifecycle’ approach to devices
- …

Guidance on cybersecurity for medical devices – MDCG 2019-16



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

Guidance on cybersecurity for medical devices – MDCG 2019-16



General safety and performance requirements with focus on cybersecurity

IT Security (sec. 17.4, 23.4ab)

Operation Security (sec. 14.1, 14.2, 17.1)

Information Security (sec. 17.2)

Safety/security and effectiveness (sec. 1)

Reduce risk to ensure intended device performance and high level of protection of health (sec. 2, 5, 6, 9)

- In all operation mode
- Intended/reasonable foreseeable risk

Basic Cybersecurity Concepts

Secure Design and Manufacture (sec. 4a)

- Risk management across the life cycle (sec. 3, 14.4, 14.5, 19.3)
- Protection against risk during intended use and reasonable foreseeable misuse (sec. 3c, 8)
- Protection against unauthorised access (sec. 17.4, 18.8)
- Identify threats, vulnerabilities, hazards, risks (sec. 3b)
- Establish risk control measures (sec. 4)
- Minimum IT security requirements (sec. 17.4, 14.5)

Verification/validation (sec. 17.2)

Acceptable residual risk (sec. 4)

Documentation* (sec. 3)

Regular updates

State of the art (sec. 1, 4, 17.2)

MDR Annex I

Information for users, instructions and labelling (sec. 4, 23.1, 22.1, 23.4)

* See also Annex II of MDR

Security risk vs safety related risk

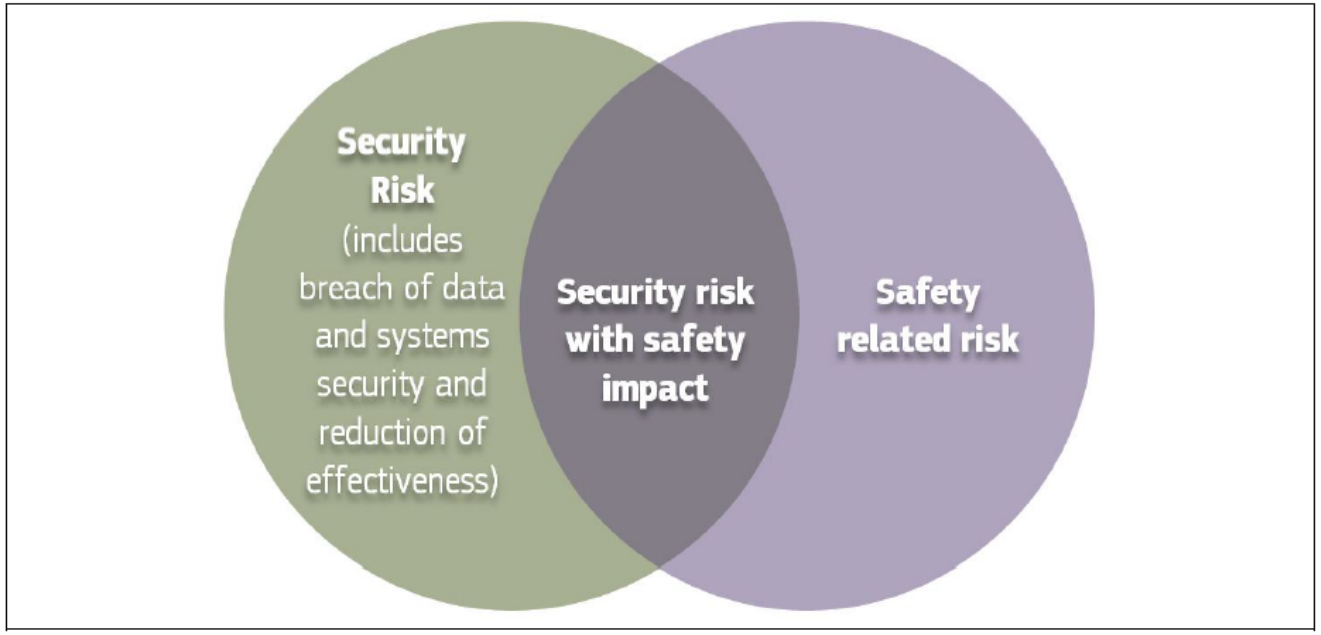
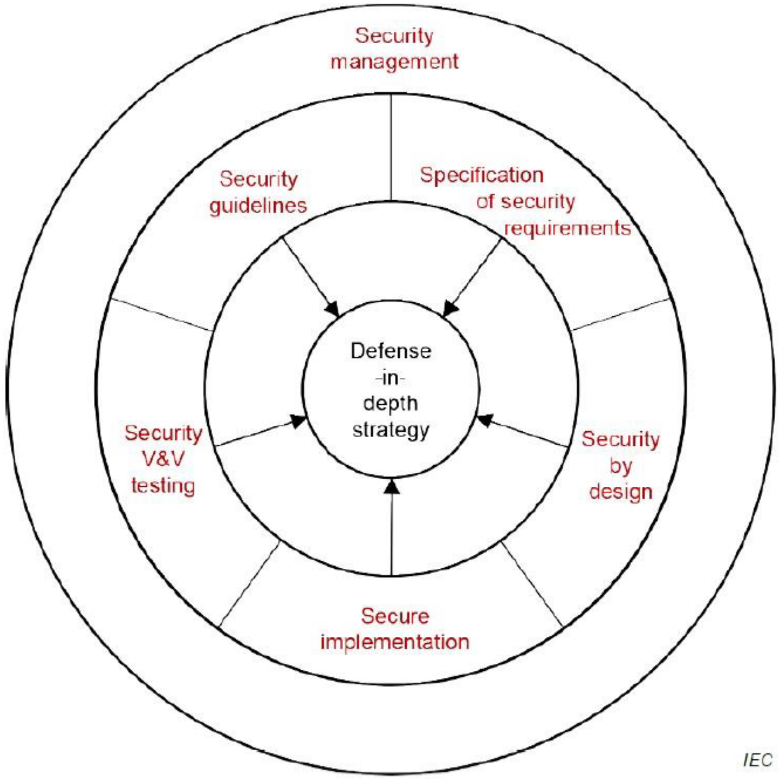

Security Risk (includes breach of data and systems security and reduction of effectiveness)
Security risk with safety impact
Safety related risk

Figure 3: Cybersecurity measures may cause safety impacts

Secure by design and lifecycle approach



IEC

Post–Market Surveillance and Vigilance

- **Post-Market Surveillance of a medical device's life cycle**
  - ❑ operation of the device in the intended environment
  - ❑ sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors
  - ❑ vulnerability remediation
  - ❑ incident response
- **Vigilance**
  - ❑ responsibility for reporting all serious incidents and field safety corrective actions (FSCA).
  - ❑ Field safety notices (FSN) so that to ensure required actions are followed and completed in a timely manner.

European
Commission

Joint Responsibility

European
Commission

Conclusion