Cybersecurity in medical devices

The perspective from the Notified body

Peter Kramar, PhD

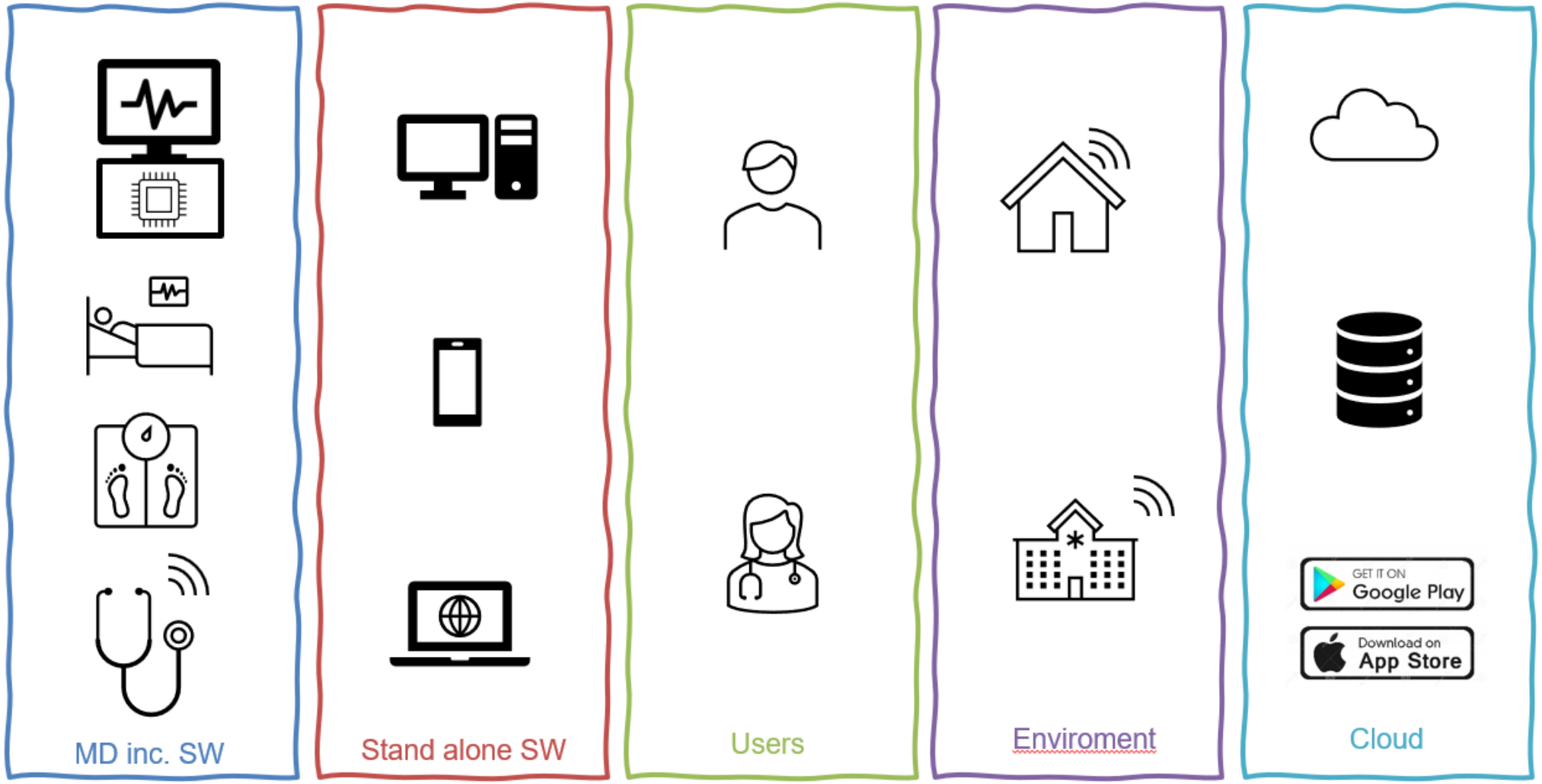
Top New Technologies That Will Impact Healthcare In Future

1. Personal Health Assistants
2. Analytics Of Health Data
3. Organ-on-a-chip Technology
4. Gene Editing
5. Internet Of Medical Things (IoMT)
6. Robotics In Surgery
7. 3D Bioprinting
8. Augmented Reality(AR) In Clinical Training
9. Virtual Reality(VR) In Therapy
10. Health Wearables For Elderly People

Top New Technologies That Will Impact Healthcare In Future

1. **Personal Health Assistants**
2. **Analytics Of Health Data**
3. Organ-on-a-chip Technology
4. Gene Editing
5. **Internet Of Medical Things (IoMT)**
6. **Robotics In Surgery**
7. 3D Bioprinting
8. **Augmented Reality(AR) In Clinical Training**
9. **Virtual Reality(VR) In Therapy**
10. **Health Wearables For Elderly People**

MD Software type combinations



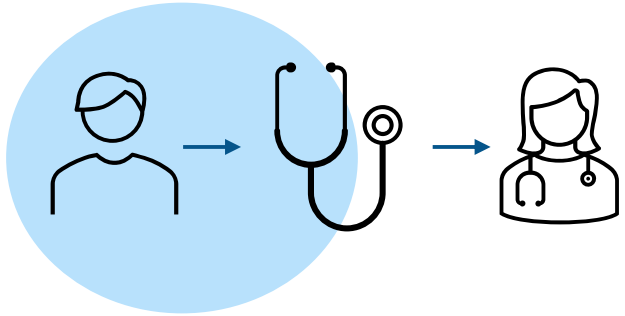
Standards related to medical device software

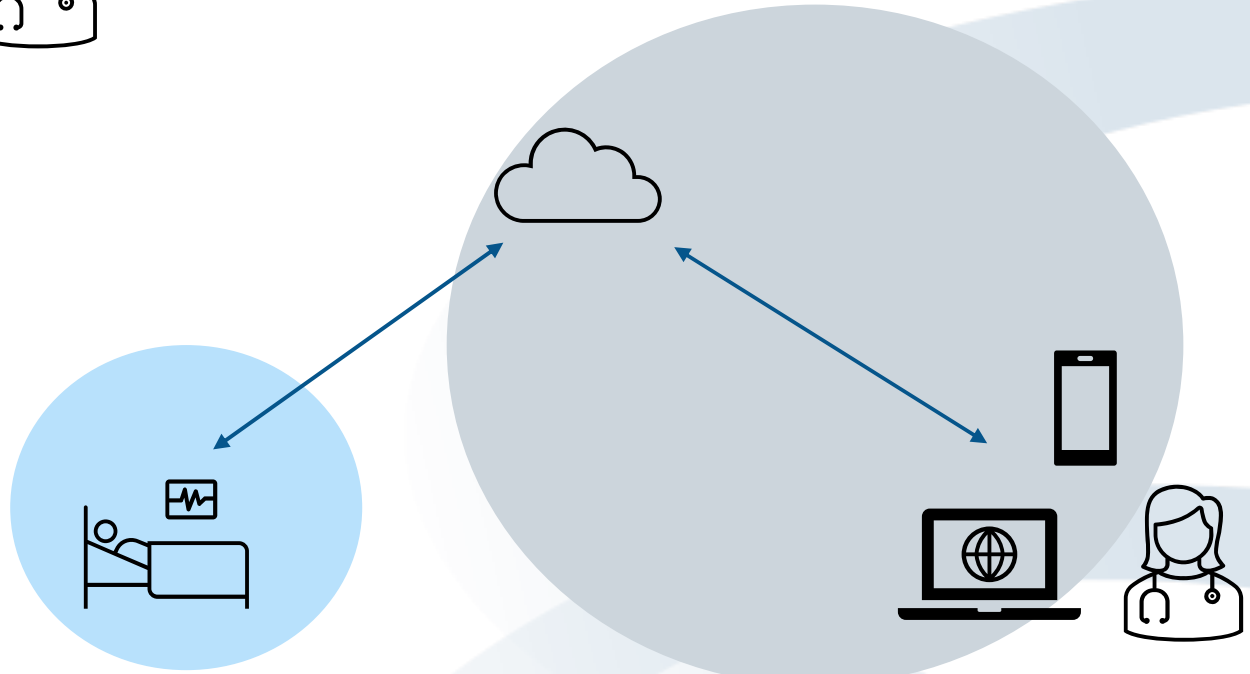
- **ISO 13485:2016** Medical devices - Quality management systems - Requirements for regulatory purposes
- **ISO 14971:2019** Medical devices — Application of risk management to medical devices
- **IEC 62304:2006+A1:2015** – medical device software – software life cycle processes
- **IEC 60601-1:2006/A2:2021** Medical Electrical Equipment Medical electrical equipment - Part 1: General requirements for basic safety and essential performance (clause 14)
- **IEC 82304-1:2016** Health software Part 1: General requirements for product safety
- **IEC 81001-5-1:2021** Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle.
- **IEC/TR 80002-1:2009** Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software

Guidelines related to SW

- **MDCG 2020-1** Guidance on clinical evaluation (MDR) / Performance evaluation (IVDR) of medical device software
- **MDCG 2019-16 rev.1** Guidance on cybersecurity for medical devices
- **MDCG 2019-11** Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746
- **MDCG 2018-5** UDI assignment to medical device software

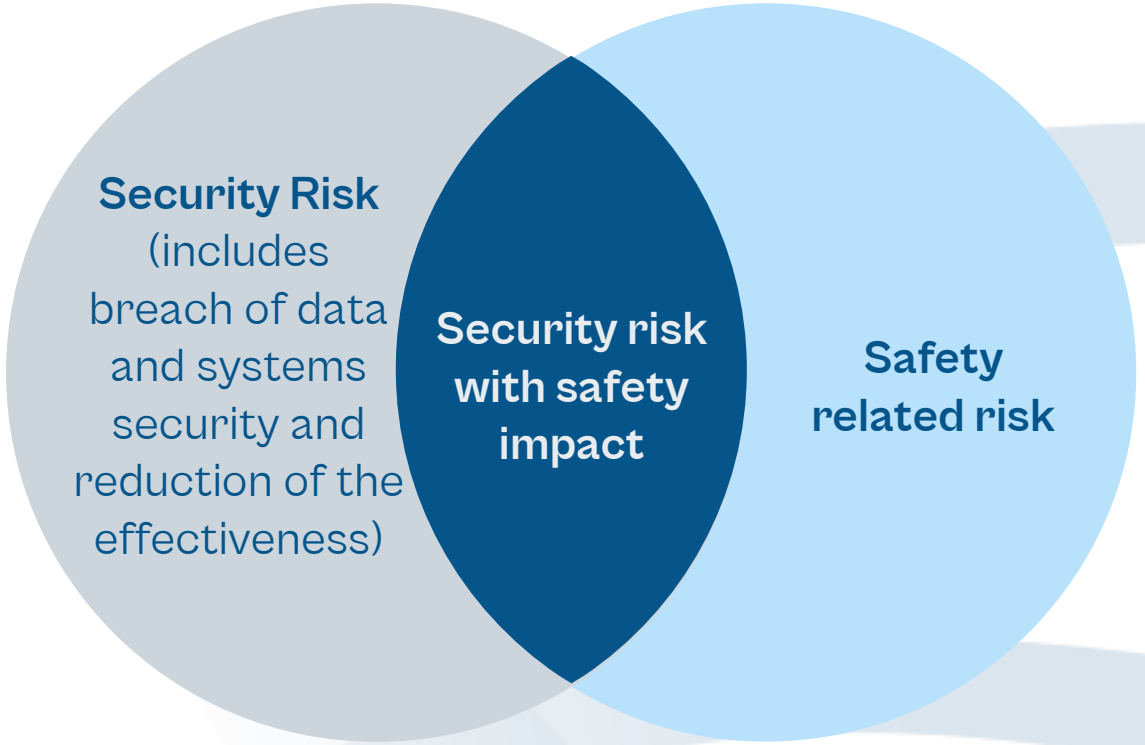
Safety - Security





Security - Cybersecurity

State where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to violation of confidentiality, integrity and availability are maintained at an acceptable level through life cycle Source ISO 81001-1:2021 [3.2.13]



MDCG 2019-16 rev. 1

Security - Cybersecurity

Hackers Can Remotely Access Syringe Infusion Pumps to Deliver Fatal Overdoses!

75% of infusion pumps have cyber flaws, putting them at risk from hackers: study

Published March 3, 2022

Source: https://www.medtechdive.com/news/infusion-pumps-cyber-flaws-at-risk-hackers-bd-baxter/619735/#:~:text=Three%20out%20of%20four%20infusion,Unit%2042%20threat%20research%20service.

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

Source: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

„The hype“ of Cybersecurity

- **Healthcare** continues to **experience the highest data breach costs of all industries**, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. (source: IBM)
- **The healthcare** sector **suffered nearly 337 breaches** in the first half of 2022 alone, **affecting 19,992,810 individuals.** (source: Protenus)
- **Healthcare email fraud** has **increased by 473%** since 2019 (source: HIPAA Journal)
- **Over 93% of healthcare organizations have experienced a data breach in recent years, and 57% have had more than five data breaches.** (source: Black Book Research)
- **The cost of a healthcare breach** is about **$408 per patient record**, without including the cost of the loss of business, productivity and reputation. (source: Healthcare Finance News)
- **Medical devices have** an average of **6.2 cyber security vulnerabilities each.** (source: Cybersecurity Ventures)

Timeline of Cybersecurity for medical devices

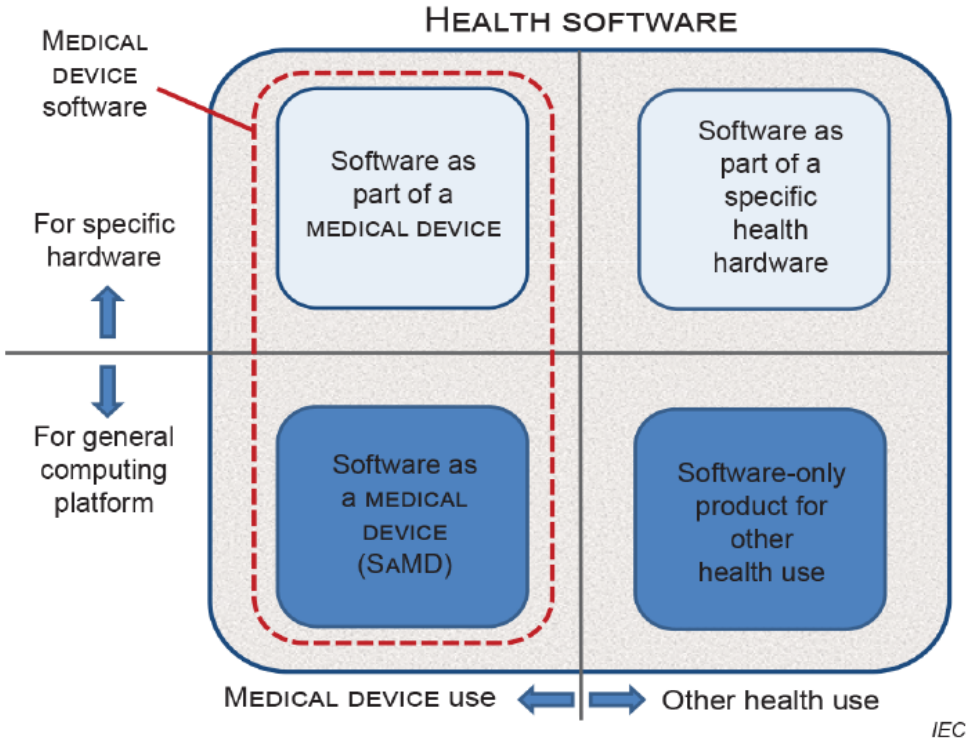
- MDD: 1 sentence indirectly referring to (cyber)security
- MDR: 4 paragraphs on cybersecurity
- MDCG 2019-16: 47 pages of cybersecurity requirements
  - Non-biding
  - Lack of clear requirements
- IEC 81001-5-1: 56 pages
  - Clear requirements
  - EU: Harmonized in near future
  - Already Recognized Consensus Standard by FDA, Same all over the world

MDR requirements related to Cybersecurity

Annex I
GENERAL SAFETY AND PERFORMANCE REQUIREMENTS

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.

IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle.



4 General requirements

5 Software development PROCESS

6 SOFTWARE MAINTENANCE PROCESS

7 SECURITY RISK MANAGEMENT PROCESS

8 Software CONFIGURATION MANAGEMENT PROCESS

9 Software problem resolution PROCESS

MDR requirements related to Cybersecurity

MDR (EU) 2017/745

MD Technical documentation

- **Annex I (17.2)**
- **Software lifecycle**
  IEC 62304:2006+A1:2015
- **Seurity risk management**
  ISO 14971:2019
- **Usability**
  IEC 62366-1:2015

Organization QMS

- **ISO 13485:2016**
  - Periodic reviews
  - Human resources
  - Purchase/Infrastructure
  - Design and Development
  - Continuous improvement

- **IEC 81001-5-1:2022**

Implementation of Cybersecurity in Organization QMS

IEC 81001-5-1:2022	ISO 13485:2016
4.1.1 Quality management system	
4.1.2 Identification of responsibilities	
4.1.3 Identification of applicability	
4.1.4 SECURITY expertise	**6.2**
4.1.5 SOFTWARE ITEMS from third-party suppliers	**7.4**
4.1.6 Continuous improvement	**8.5**
4.1.7 Disclosing SECURITY-related issues	**7.3.2**
4.1.8 Periodic review of SECURITY defect management	**5.6**
4.1.9 ACCOMPANYING DOCUMENTATION review	**7.3**
4.2 SECURITY RISK MANAGEMENT	
4.3 SOFTWARE ITEM classification relating to risk transfer	**7.4**

Thank you