Bundesministerium
für Gesundheit

Regulatory Views on Medical Devices Cybersecurity in the European Union

DITTA Workshop on Cybersecurity

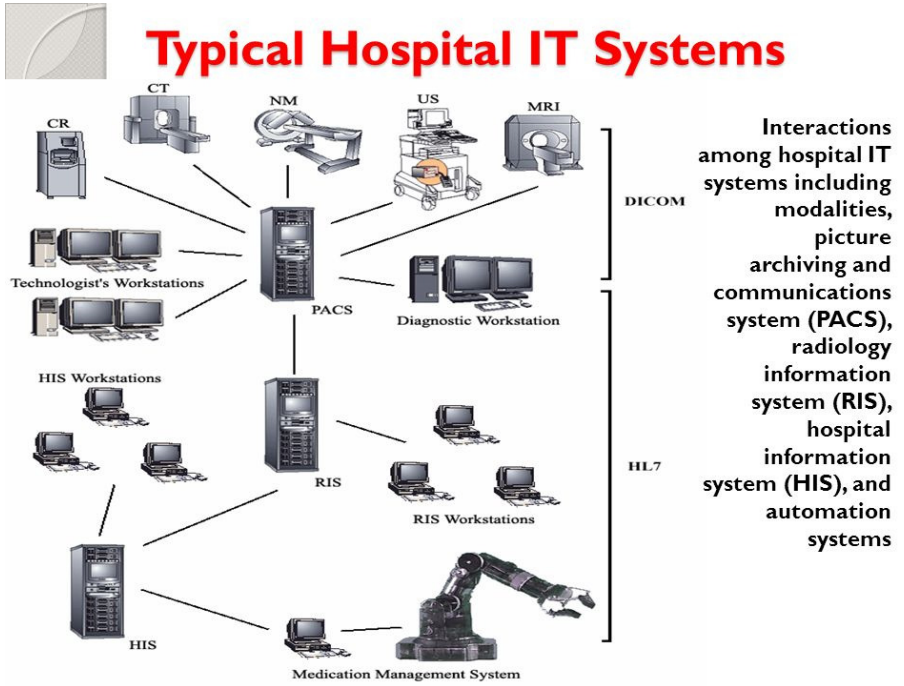
1. **Medical Devices Cybersecurity**
2. **Legal requirements**
3. **Ongoing/Started Activities**
4. **Expectation of regulators**

Cybersecurity and Medical Devices?

Cybersecurity, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.
Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators, whether intentional or accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods

Safety and Performance of Medical Devices depend on
Cybersecurity of the IT environment in which the MD performs
Cybersecurity of the MD

Cybersecurity of medical devices = Cybersecurity of Hospital IT Systems



Cybersecurity of hospital IT systems is very much focussed on data integrity, data protection, ensuring functionality etc.

Cybersecurity of medical device is more focussed on ensuring safety and performance

Cybersecurity Threats

Medical device companies and healthcare organizations face an array of cyber threats including untargeted and increasingly sophisticated targeted attacks. Threats may include:

- Disruption of care/service (including potential for patient deaths)
- Deception of staff with spoof email or fake websites to obtain login credentials or install malware
- Unintentional or intentional 'Insider threat', which can pose a significant threat due to the position of trust within an organization
- Loss of patient information – especially electronic protected health information (ePHI)
- Data breach, information exfiltration and loss of assets
- Blackmail, extortion and duress through exploitation of exfiltrated sensitive data
- Intellectual Property (IP) theft

Healthcare cybersecurity continues to focus on the protection of patient health records, whilst failing to address the real threats to, or adequately protect patient health

Legal requirements on cybersecurity for medical devices

New Medical Devices Regulation

Lifecycle process Risk management

Manufacturers shall establish, implement, document and maintain a risk management system. Risk management shall be understood as a continuous iterative process throughout t**he entire lifecycle of a device, requiring regular systematic updating**. In carrying out risk management manufacturers shall:

(a) establish and document a risk management plan for each device;
(b) identify and analyse the known and foreseeable hazards associated with each device;
(c) estimate and evaluate the risks associated with, and occurring during, the intended use and **during reasonably foreseeable misuse;**
(d) **eliminate or control the risks** referred to in point (c) in accordance with the requirements of Section 4;
(e) evaluate the impact of information from the production phase and, in particular, **from the post-market surveillance system,** on hazards and the frequency of occurrence thereof, on estimates of their associated risks, as well as on the overall risk, benefit-risk ratio and risk acceptability; and
(f) based on the evaluation of the impact of the information referred to in point (e), if necessary amend control measures in line with the requirements of Section 4.

Legal requirements on cybersecurity for medical devices

MDR Annex I (partially) new specific requirements on “software or software driven MD”

14.2 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;

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.

Legal requirements on cybersecurity for medical devices

MDR Annex I (partially) new specific requirements on “software or software driven MD”

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.

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.

Legal requirements on cybersecurity for medical devices

MDR Annex III Postmarket Surveillance by the manufacturer

(a) The post-market surveillance plan shall address the collection and utilization of available information, in particular:

– information concerning serious incidents, including information from PSURs, and field safety corrective actions;
– records referring to non-serious incidents and data on any undesirable side-effects;
– information from trend reporting;
– relevant specialist or technical literature, databases and/or registers;
– information, including feedbacks and complaints, provided by users, distributors and importers; and
– publicly available information about similar medical devices.

Legal requirements on cybersecurity for medical devices

MDR Annex III Postmarket Surveillance by the manufacturer

(b) The post-market surveillance plan shall cover at least:

- **a proactive and systematic process** to collect any information referred to in point (a). The process shall allow a correct characterisation of the performance of the devices and shall also allow a comparison to be made between the device and similar products available on the market;
- effective and appropriate methods and processes to assess the collected data;
- suitable indicators and threshold values that shall be used in the **continuous reassessment of the benefit- risk analysis and of the risk management** as referred to in Section 3 of Annex I;
- effective and appropriate methods and tools to investigate complaints and analyse market-related experience collected in the field; …….

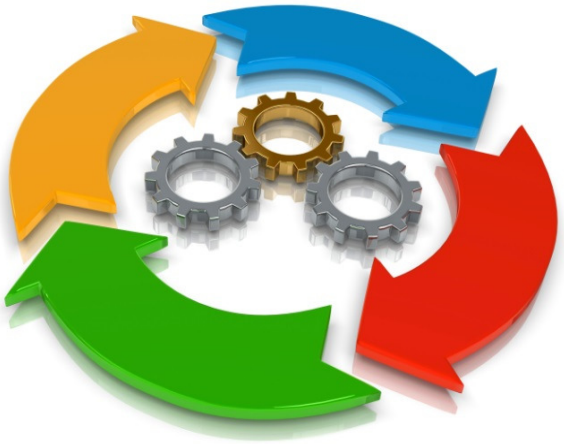
….

Ongoing activities

- **US-Based National Health information and Analysis Center workshop in May 2018; Internet of Things (IoT); US Diabetes Device Security**
- **Discussion Joint Meeting between Medicine and Devices Heads Strategic Group; FDA standard UL2900 + guidance of pre- and post-market management of cyber security**
- **Ongoing project on cybersecurity undertaken in 2017 by some companies in Finland**
- **Germanys BSI (Bundesamt für Sicherheit in der Informationstechnik) and ZVEI draft of requirements published May 2018; FDA requires a report based on ISO/IEC 2701; Germans law on cyberattack; SE+IE+FR have initiatives for health providers; necessary to clarify the potential of overlap.**
- **Several more …. but mainly related to IT security – data protection only**

Our proposal

A **voluntary European** cybersecurity certification **framework....**



...to enable the creation of tailored EU cybersecurity certification schemes for ICT products and services...

...that are valid across the EU

Bundesministerium
für Gesundheit

European Commission

State of Play and next steps

Proposal adopted by the Commission in September 2017.

Currently in negotiations with the co-legislators

- Discussions on the proposal have begun in the Council
- Draft reports published by IMCO and LIBE Committees of the European Parliament.

Goal: agreement before Q2 2019.

"Once the Framework is established, the Commission will invite the relevant stakeholders to focus on three priority areas":

- Security in critical or high-risk applications.
- Cybersecurity in widely-deployed digital products, networks, systems and services such as email encryption, firewalls and Virtual Private Networks.
- **"Security by Design" in** low-cost, digital, interconnected mass consumer devices which make up the Internet of Things. For example:
  - Secure development methods including adequate security testing.
  - Updates in the event of newly discovered vulnerabilities or threats.

Expectations from MD regulators

- Cybersecurity by design and as continuous lifecycle process
- Realistic balance between MD manufacturers and IT network owner requirements
- Post-market surveillance process must also cover Cybersecurity aspects (analysis of threats, analysis of vulnerabilities, corrective actions (if necessary together with the IT network owner)