TIC COUNCIL

THE INDEPENDENT VOICE OF TRUST

TIC Council Webinar

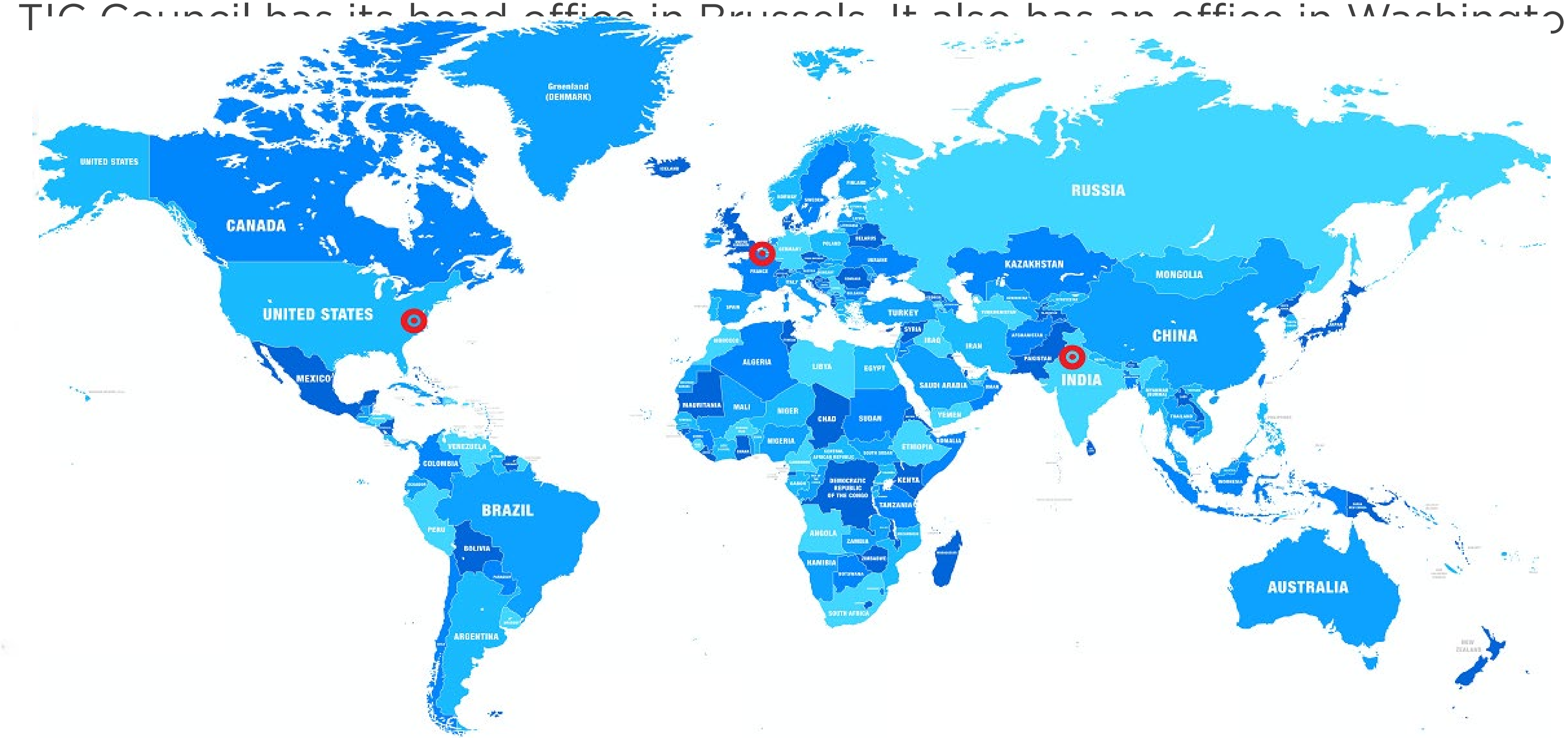
TIC Sector and the Cybersecurity of Medical Devices in Europe

23 July 2020

TIC Council

The Independent Voice of Trust

- Born from the merger of IFIA and CEOC
- ~90-member companies & organizations active in more than 160 countries (HQ mapped)
- TIC Council has its head office in Brussels. It also has an office in Washington and



TIC Council Mission

As the voice of the global independent testing, inspection and certification industry, the TIC Council engages governments and key stakeholders to advocate for effective solutions that protect the public, support innovation and facilitate trade.

The TIC Council works with its members to promote best practices in safety, quality, health, ethics and sustainability

TIC COUNCIL
Independent Voice of Trust

Webinar

TIC SECTOR AND THE CYBERSECURITY OF MEDICAL DEVICES IN EUROPE

23 July 2020 15:00

Anna-Eva Ampelas,
Head of Unit for Medical Devices and
Hospital Based Health Technology
Assessment, DG SANTÉ,
European Commission

Dr. Abtin Rad,
Global Director Functional Safety,
Software and Digitization, Active
Medical Products, TÜV SÜD

Dr. Georg Heidenreich,
Chairman of IEC/CD 80001-5-1,
International Organisation
of Standards

Commission update

TIC Council webinar – Cybersecurity of medical devices

Directorate-General for Health and Food Safety (DG SANTE)

Anna-Eva AMPELAS – Head of Unit B.6 on Medical Devices and Health Technology Assessment

Health

Agenda

1. COVID-19 and MDR/IVDR Implementation
2. Impacts of the new Regulations (MDR/IVDR) on cybersecurity of medical devices and regulators' expectations
3. How should manufacturers consider interface between MDR/IVDR and other regulations (such as the GDPR)?

1) COVID-19 and MDR/IVDR implementation

1) COVID-19 and MDR/IVDR implementation

- MDR postponement of application date
- Ramping up of production
- European Standards made freely available
- Numerous COVID-19 related guidance published
- Combatting export restrictions
- Derogations
- Joint procurement Agreement
- Clearing House

Regulation (EU) 202/561 and main consequences

- Regulation (EU) 2020/561 adopted on 23 April 2020 **amending MDR**, as regards the **dates of application** of certain of its provisions

- Commission Implementing Regulation (EU) 2020/666 of 18 May 2020 amending Implementing Regulation (EU) No 920/2013 as regards the renewal of **designations** and the **surveillance and monitoring of notified bodies**

- Commission Recommendation (EU) 2020/403 of 13 March 2020 on **conformity assessment and market surveillance** procedures within the context of the COVID-19 threat

MDCG guidance and other COM documents published COVID-19 (I)

- MDCG Guidance on temporary extraordinary measures related to medical device **notified body audits** during COVID-19 quarantine orders and travel restrictions
- MDCG Guidance on the **renewal of designation and monitoring of notified bodies** under Directives 90/385/EEC and 93/42/EEC to be performed in accordance with Commission Implementing Regulation (EU) 2020/666 amending Commission Implementing Regulation (EU) 920/2013
- Guidance on how to check if medical devices and PPE can be **lawfully placed on the EU market** and thus purchased and used
- Commission guidelines on the adoption of **Union-wide derogations** for medical devices

MDCG guidance and other COM documents published COVID-19 (II)

- MDCG Guidance on regulatory requirements for **ventilators** and related accessories
- Communication from the Commission concerning Guidelines on COVID-19 **in vitro diagnostic tests** and their performance
- Working document of Commission services on **performance of** COVID-19 **test methods** and devices and proposed performance criteria
- **Database** of devices and publicly available **performance data COVID-19 In Vitro Diagnostic Devices and Test Methods**
- Guidance on Medical devices, Active implantable medical devices and in vitro diagnostic medical devices **in the COVID-19 context**

MDCG guidance and other COM documents published COVID-19 (III)

- Guidance to increase production of safe medical supplies (**PPE, hand gel, 3D printing)**
- Guidance on **face masks**
- IMDRF Standards Checklist modified in scope of COVID-19
- Q&A on **conformity assessment procedures** for protective equipment
- New lists of **harmonised standards** made available for medical devices
- European standards for medical supplies made freely available to facilitate increase of production
- Standardisation request in support of the new Regulations on medical devices
- Commission recommendation on **conformity assessment and market surveillance procedures**

MDR/IVDR Implementation – Published Guidance

March 2020

- ✓ Update of guidance on implant card
- ✓ Transitional provisions of article 120 (3) and (4) for class I medical device
- ✓ Significant changes regarding transitional provisions in Art.120
- ✓ Clinical evaluation/ Performance evaluation of medical device software

April 2020

- ✓ Update of guidance on Article 54(2)b
- ✓ PMCF templates
- ✓ Sufficient clinical evidence for legacy devices
- ✓ Clinical evaluation – Equivalence

May 2020

- ✓ Safety reporting in clinical investigations

June 2020

- ✓ Consultations of authorities on devices with ancillary substances and TSE susceptible tissues
- ✓ Update of guidance on UDI for sytems and procedure packs

July 2020

- ✓ Clinical evaluation assessment report template

MDR/IVDR Implementation

Expert panels

- Establishment of expert panels and reference labs (ongoing). Act on design. of expert panels 10.9 2019.
- Rolling Plan 3 June 2020

Implementing Acts: for information

More than 80 empowerments for implementing and delegated acts (including Common Technical Specifications – CS)(of which 18 mandatory)

Next in line for MD:

- Common specifications on reprocessing of single-use devices (Q3 2020)
- Common specifications of devices without medical purpose (Q4 2020)
- EUDAMED impl. Act (Q4 2020)

MDR/IVDR Implementation

Implementing Acts: for information: Standardisation supporting the new Regulations

- Standardisation Request (Commission Implementing Decision with Annexes) according to Art. 10 of the Standardisation Regulation (EU) 1025/2012
- Committee on Standards (Member States representatives) expressed a positive opinion
- Commission adopted an Implementing Decision on 15 May 2020 and notified it to CEN and CENELEC.
- CEN and CENELEC rejected the Request on 16 June 2020 which can result in a lack of legal basis for the standardisation work in support of MDR and IVDR and for the publication of references to standards in the OJEU under MDR/IVDR. Could lead to increased use of Common specifications.

IVDR Specific

Current main items

- Setting up of reference laboratories (Q3 2020/Q1 2021) – can be designated after 25 November 2020
  - Implementing act on tasks and criteria
  - Implementing act on fees
  - Call for application
- Transposing Common Technical Specifications into Common specifications for IVD Class D (Q3 2020)
- Developing new Common Specifications
- Guidance on classification – finalisation imminent

2) Impacts of the new Regulations (MDR/IVDR) on cybersecurity of medical devices and regulators' expectations

2) Impacts of the new Regulations (MDR/IVDR) on cybersecurity of medical devices

- New regulations bring about an increased expectations for all types of medical devices including those incorporating software, as well as 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
- …

General Safety and Performance Requirements (GSPR): Annex I - cybersecurity of medical devices

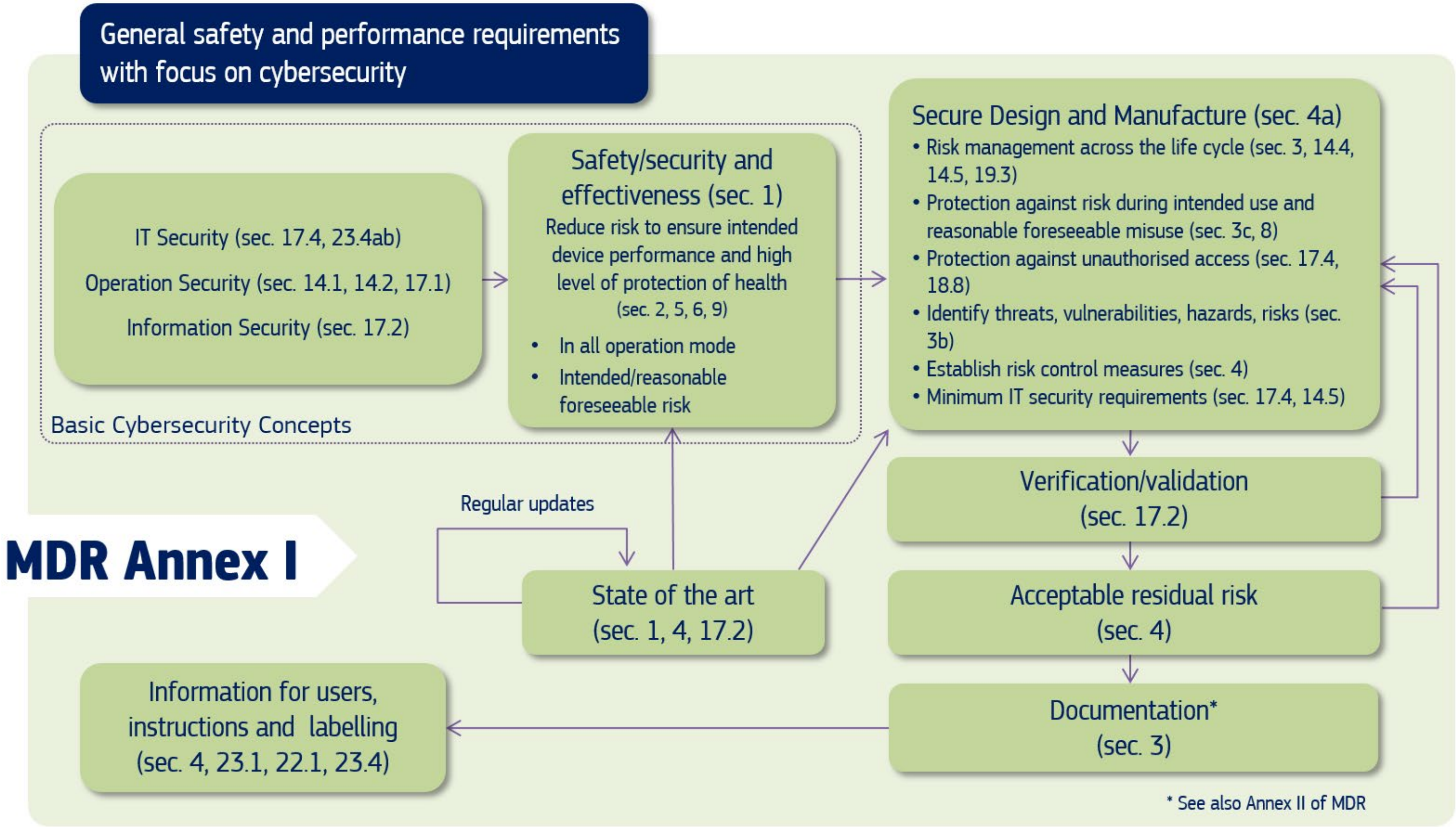
- Specification of Cybersecurity Requirements included in Annex 1 of the MDR
- IT Security
- Information Security
- Operations Security
- Safety, Security and Effectiveness
- State of the Art
- Safe Design and Manufacture
- Risk Control Measures
- Verification and validation
- Risk-benefit analysis: assessing the acceptability of risk
- Documentation
- Information & labelling

2) Impacts of the new Regulations (MDR/IVDR) on cybersecurity of medical devices – cont.

- MDCG guidance specific to software

Reference	Title	Publication
MDCG 2020-1	Guidance on clinical evaluation (MDR) / Performance evaluation (IVDR) of medical device software	March 2020
MDCG 2019-11	Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746	October 2019
MDCG 2019-16	Guidance on cybersecurity for medical devices	December 2019

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)

MDR Annex I

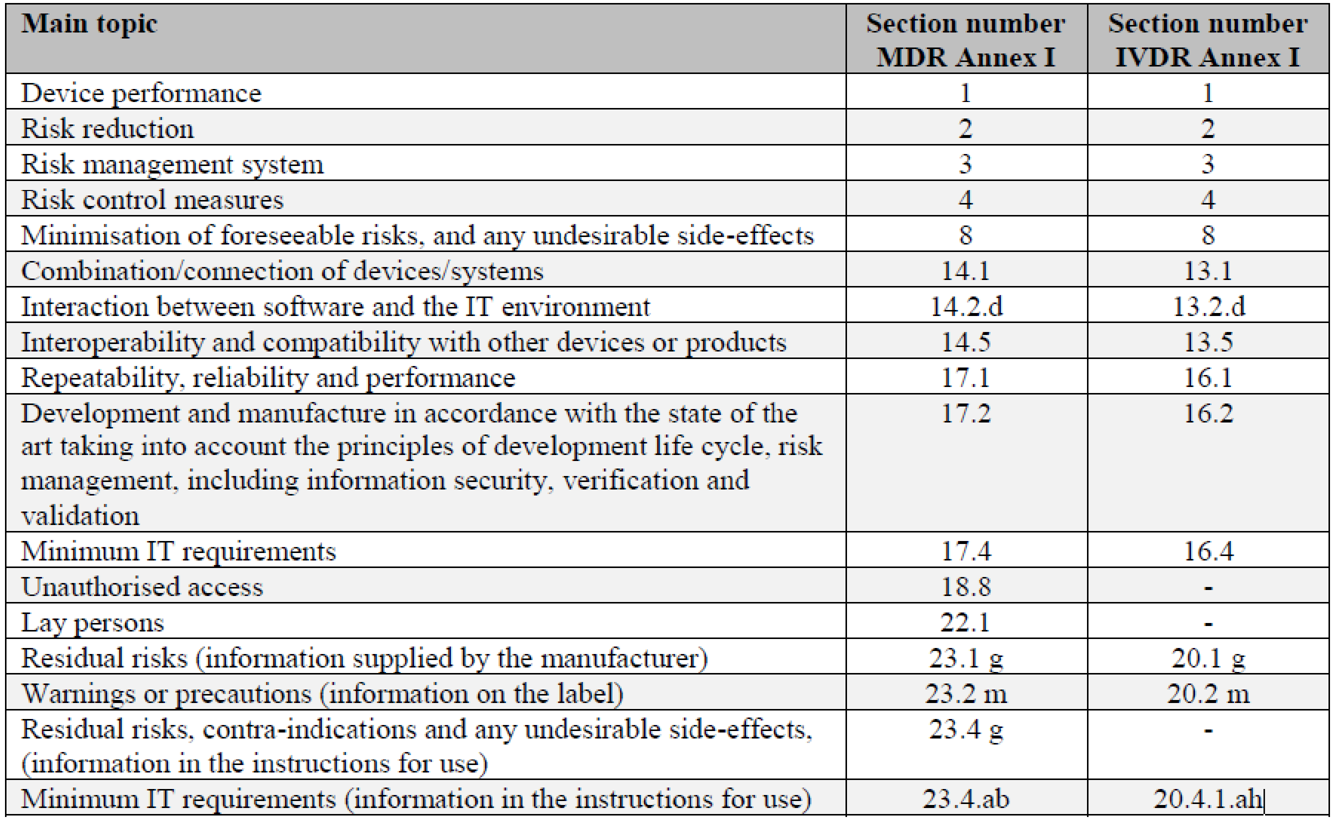
Regular updates

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

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

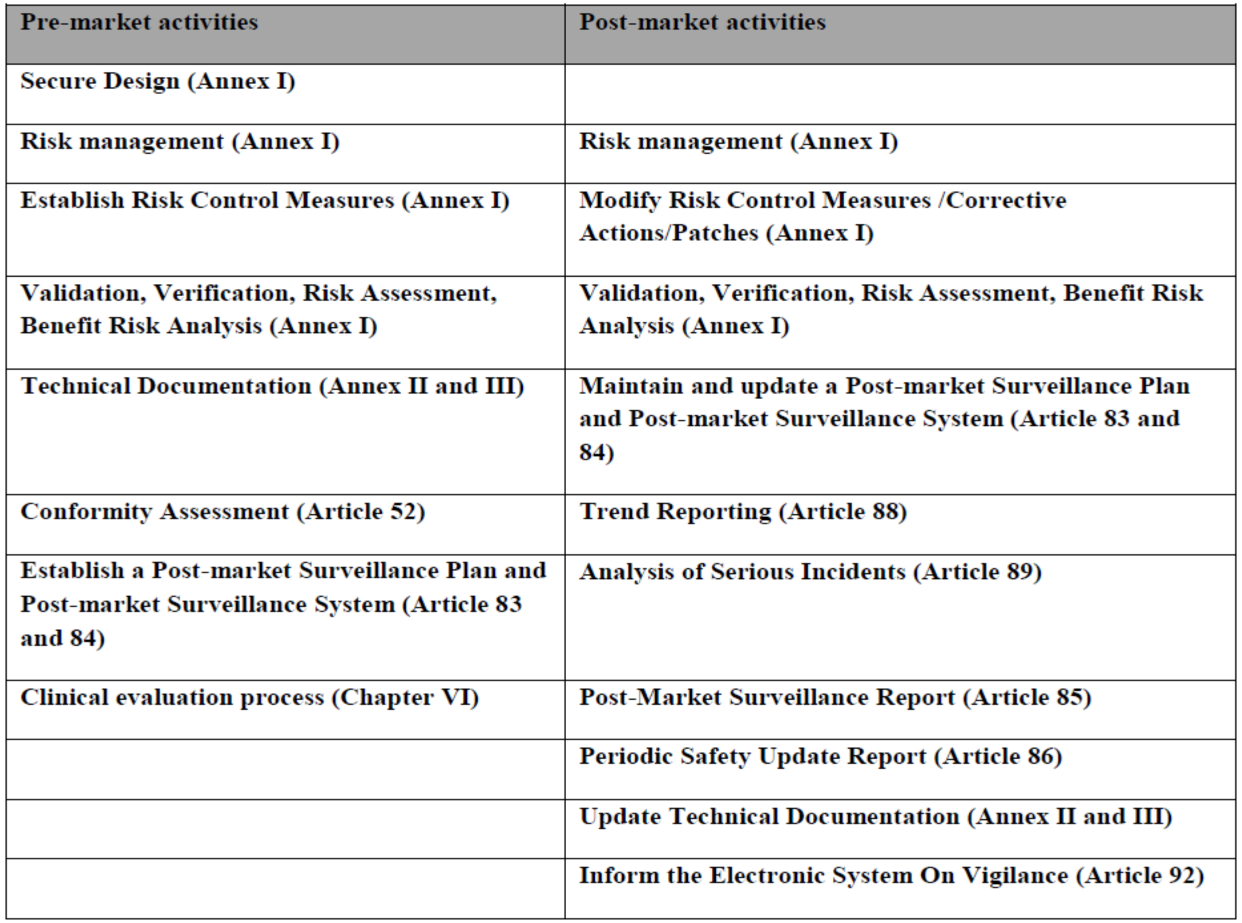
* See also Annex II of MDR

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 – a lifecycle approach



Pre-market activities	Post-market activities
Secure Design (Annex I)	
Risk management (Annex I)	Risk management (Annex I)
Establish Risk Control Measures (Annex I)	Modify Risk Control Measures /Corrective Actions/Patches (Annex I)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)	Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)
Technical Documentation (Annex II and III)	Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Conformity Assessment (Article 52)	Trend Reporting (Article 88)
Establish a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)	Analysis of Serious Incidents (Article 89)
Clinical evaluation process (Chapter VI)	Post-Market Surveillance Report (Article 85)
	Periodic Safety Update Report (Article 86)
	Update Technical Documentation (Annex II and III)
	Inform the Electronic System On Vigilance (Article 92)

Guidance on cybersecurity for medical devices – MDCG 2019-16

- **IT Security, Information Security, Operation Security**

Annex I of the Medical Devices Regulations explicitly sets out the requirement for manufacturers of in vitro diagnostic medical device and medical device to fulfil minimum requirements concerning hardware, IT networks3 characteristics and IT security measures, including protection against unauthorised access. All these requirements are necessary in order to run the software as intended

- **Safety, Security and Effectiveness**

Information security and IT security are addressed explicitly in Annex I 17.2 (MDR), 17.4 (MDR), 18.8 (MDR), 16.2 (IVDR) and 16.4 (IVDR) whereas "Safety and Effectiveness" issues are addressed in section 1 of Medical Devices Regulations Annex I

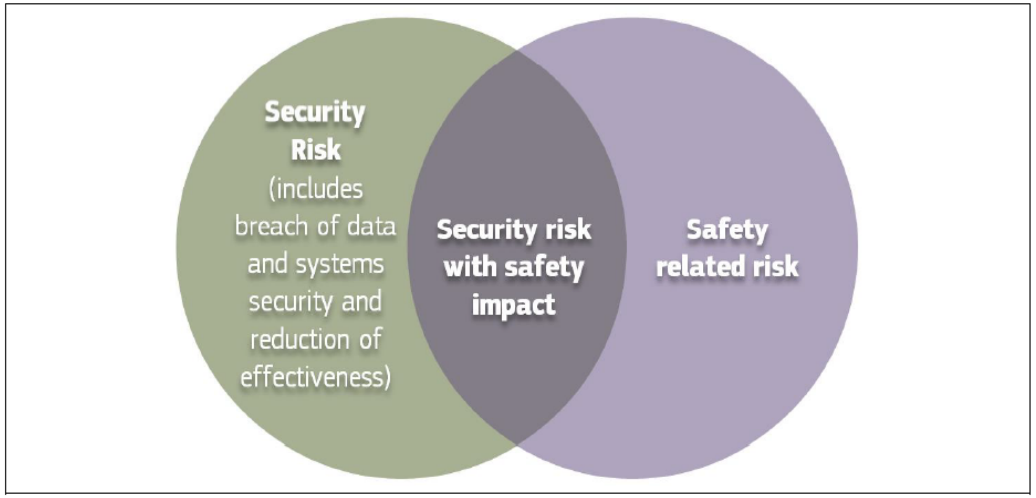

Security Risk (includes breach of data and systems security and reduction of effectiveness)
Security risk with safety impact
Safety related risk

Figure 3: Cybersecurity measures may cause safety impacts

Guidance on cybersecurity for medical devices – MDCG 2019-16

- **Intended use and intended operational environment of use**

Manufacturers determine design inputs to ensure safety and effectiveness of products against cybersecurity risks and threats. This should be considered in accordance with the nature of the device, including the device type and intended communication technologies usage. A medical device should be designed in a layered defence in depth approach and therefore should not rely on security controls in the operating environment.

- **Reasonably foreseeable misuse**

Medical device manufacturers should ensure that a medical device is designed and manufactured in a way that ensures that the risks associated with reasonably foreseeable environmental conditions are removed or minimised. This may include the infield monitoring of the software’s vulnerabilities and the possibility to perform a device update through, for example delivering patches.

During the risk management process, the manufacturer should foresee or evaluate the potential exploitation of those vulnerabilities that may be a result of reasonably foreseeable misuse

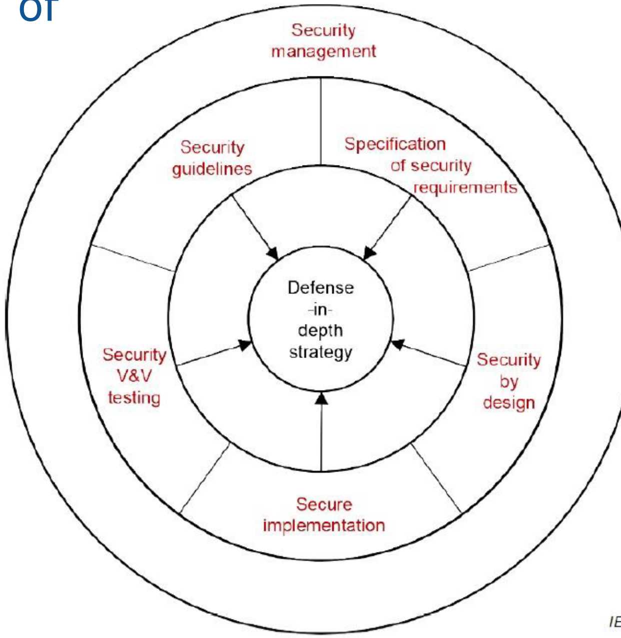
Guidance on cybersecurity for medical devices – MDCG 2019-16

- **Joint Responsibility - Specific expectations from other stakeholders**

While the MDR and the IVDR provide legal obligations only with regard to manufacturers, however it should be noted that for the provision of secured healthcare services, it is important to recognise the roles and expectations of all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators. All of these actors share responsibilities for ensuring a secured environment for the benefit of patients' safety.

- **Secure Design and Manufacture – Secure by design and lifecycle aspects**

Safety, security and effectiveness are critical aspects in the design of security mechanisms of medical devices. Therefore, there is a clear requirement that these aspects need to be considered by the manufacturers from an early stage of development and manufacturing process and throughout the entire life cycle



IE

Guidance on cybersecurity for medical devices – MDCG 2019-16

- **Lifecycle Aspects**

Addressing cybersecurity risks at the design **stage** can help mitigate cybersecurity risks that could contribute to a breach in the confidentiality, a compromise in the integrity and availability of the medical device and its data, or intentional unauthorised access to the medical device and/or the network.

During the **lifetime of the device**, the manufacturer should put in place a **process to gather post-market** information with respect to the security of the device. This process should take into account:

1. Security incidents directly related to medical device software
2. Security Vulnerabilities that are related to the medical device hardware/software and the 3rd party hardware/software used with the medical device.
3. Changes in the threat landscape, including interoperability aspects

The manufacturer should evaluate the information thus gathered, evaluate the associated security and safety risk and take appropriate measures that control the risk associated with such security incidents or vulnerabilities.

Guidance on cybersecurity for medical devices – MDCG 2019-16

- **Post-Market Surveillance of a medical device's life cycle**

a crucial aspect that manufacturers shall implement as cybersecurity vulnerabilities change and evolve over time and controls implemented during pre-market activities may be inadequate to maintain an acceptable benefit-risk level. An effective and successful post-market cybersecurity surveillance program should include the following aspects:

  - ❑ 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**

The manufacturer is responsible for reporting all serious incidents and field safety corrective actions (FSCA). The manufacturers will need to carry out investigations of serious incidents related to a cybersecurity in order to provide a comprehensive description of the serious incident and involve the distributors of the device and, where applicable, the authorised representative and importers in the system, in order to obtain the information needed from the market, especially for FSCA or issued field safety notices (FSN) so that to ensure required actions are followed and completed in a timely manner.

3) How should manufacturers consider interface between MDR/IVDR and other regulations?

Cross cutting legislation

- At EU level, the following legislative acts are relevant to the cybersecurity of medical devices or to operators dealing with protecting or processing of personal data stored in medical devices and might apply in parallel to the Medical Devices Regulations:

□ Network and Information Sytems Directive (NIS)*

□ General Data Protection Regulation (GDPR)*

□ EU Cybersecurity Act

Network and Information Sytems Directive (NIS)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

- Provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
  - Member States preparedness by requiring them to be appropriately equipped,
  - Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States.
  - A culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructures, **healthcare** and digital infrastructure. Businesses in these sectors that are identified by the Member States as **operators of essential services will have to take appropriate security measures** and to **notify incidents of significant impact** to the relevant national authority.

General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data protection-regulation-gdpr-govern_en

- Regulates the processing by an **individual, a company or an organisation** of personal data relating to **individuals** in the EU. Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable are no longer considered personal data. For data to be truly anonymised, the anonymization must be irreversible.
- The GDPR protects personal data **regardless of the technology used for processing that data** – it’s technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn’t matter how the data is stored – in an IT system, through video surveillance, or on paper.

Cybersecurity Act

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

- The Framework is based on voluntary certification schemes, which are risk based on ‘Assurance Levels’. The schemes specify the evaluation process relevant for specific product categories and their assurance levels. These Assurance Levels are representative of the level of the risk associated with the intended use of the ICT product, service or process, in terms of the probability and impact of an incident.

- The Assurance Levels are split into three categories: Basic, Substantial, High.

- The Commission will take on the responsibility of assessing the efficiency of the scheme after three years of its adoption. If found unsatisfactory, the Commission may propose a legislative act for the enforcement of mandatory requirements.

Useful links and references

- Directorate-General on Health and Food Safety (DG SANTE): https://ec.europa.eu/info/departments/health-and-food-safety
- EU health policy: https://ec.europa.eu/health/policies/overview
- Medical devices sectoral website (to be transferred): https://ec.europa.eu/growth/sectors/medical-devices
- The ‘Blue Guide’ on the implementation of EU product rules: https://ec.europa.eu/docsroom/documents/18027
- CE marking: https://ec.europa.eu/growth/single-market/ce-marking/
- CEN-CENELEC Medical equipment: https://www.cen.eu/work/Sectors/Healthcare/Pages/Medicalequipment.aspx

Some questions along the medical device life-cycle

Dr. Georg Heidenreich

Siemens Healthcare GmbH

Co-Convenor JWG7

„Safe, effective and secure health software and health IT systems, including those incorporating medical devices”

Some questions along the medical device life-cycle

1. What is the relationship between Safety and Security ?

2. CIA or AIC ? Are medical devices in „office IT“ or „factory IT“ ?

3. What‘s foreseeable - when a manufacturer analyzes threats?

4. What is the perfect balance of safety, security and performance?

5. Will „process“ or „product“ matter more ?

6. Assessment : „steep way“ or „market enabler“ ?

What is the relationship between safety and security ?

www.redefininghtefaceofbeauty.com

123RF.COM

Science Photo Library

Information Security or Operations Security ?

The Brand Factory

Patrick Hendry

What is foreseeable (from the manufacturers‘ perspective) ?

Evening Standard

PxHere.com

Nutbull.com

WHDH.com

Can we „reduce risks as far as possible” ?

EU MDR, Annex I GSPR, ch. 1, clauses 2 & 4a, p. 94, OJ 5.5.2017

AmericanCarFans.com

Will we move from „product“ to „process“ ?

Appropriate certificates of successful assessment may support

Confidence in safety, security and effectiveness !

tripadvisor.de

Alamy Stock Photo

Regulation, standards and their assessment improve confidence in the use of technical systems !

TIC COUNCIL

THE INDEPENDENT VOICE OF TRUST

Cybersecurity in medical devices

Dr. Abtin Rad
TÜV SÜD Product Service Division

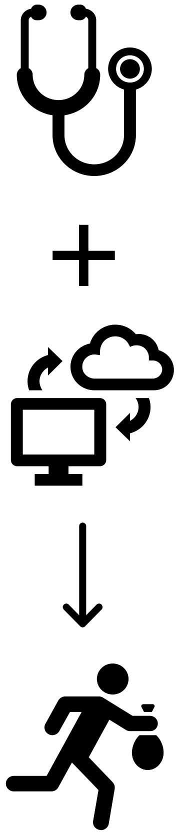
Outlook

1. Challenges and why for Cybersecurity
2. Cyber Attacks
3. Health Care Data – Data Privacy
4. Reputational damage
5. Secure Solution - safe and secure development
6. Summary

Challenges and why for Cybersecurity?

- Approximately 1 of 4 medical devices are connected medical devices
- 125 billion devices connected to the internet by 2030 [1]

- Any (medical)-device incorporating software can be vulnerable to cybersecurity threats
  - Health related risks
  - Health care data privacy related risk
  - Economic risks
  - Reputational risk



"…Cyber-attacks pose more danger to democracies and economies than guns and tanks…"
Commission President Jean-Claude Juncker 2017

Cyber Attacks

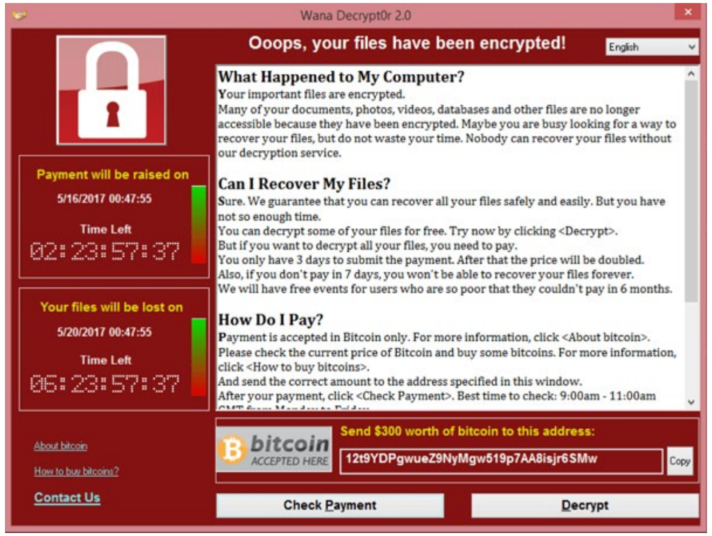
Hospira infusion pumps attack

Source: [16]

One Touch Ping insulin pump

Source: [15]

WannaCry Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

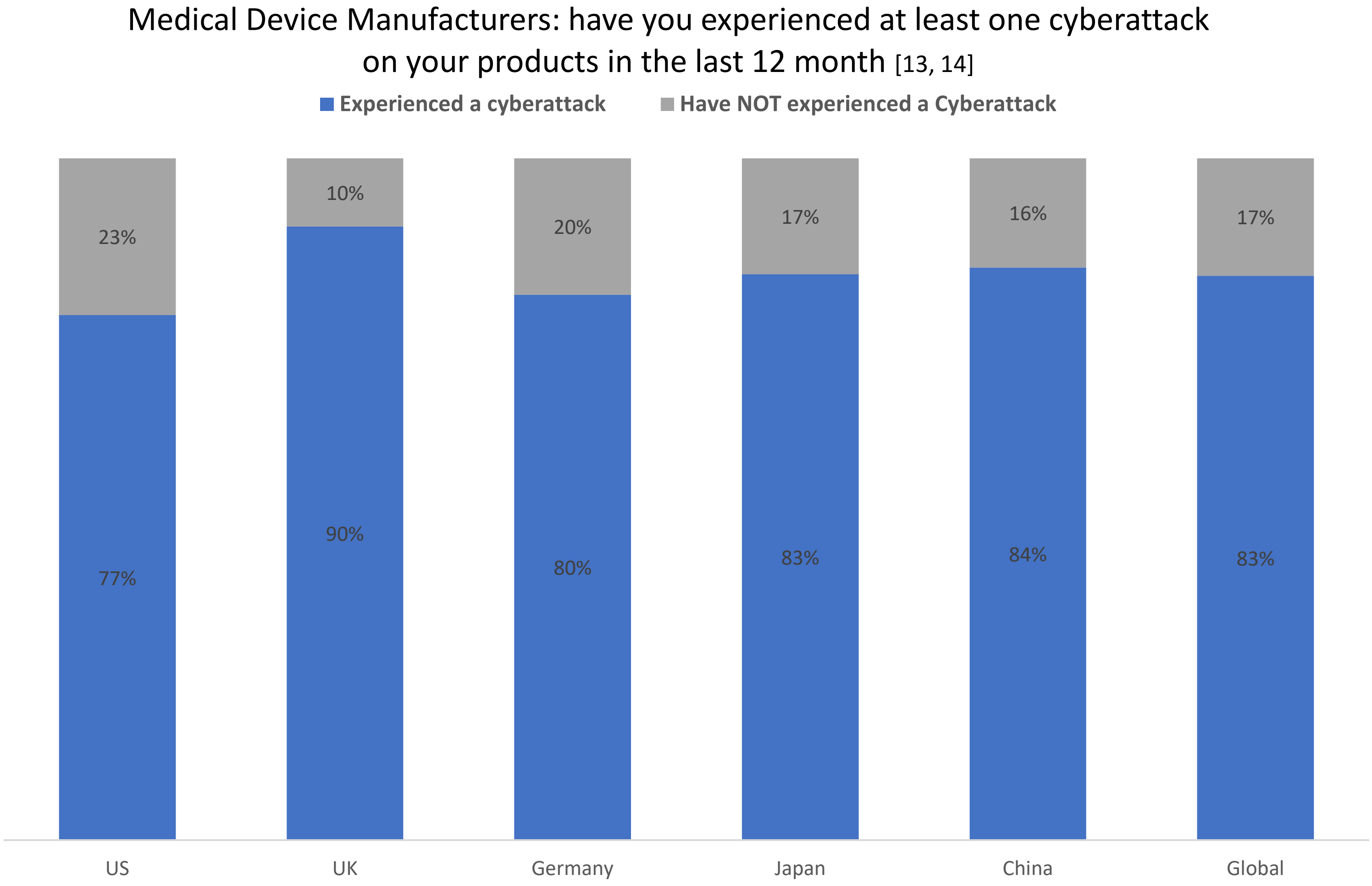
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Source: [17]

83% of medical device manufacturers hacked at least once in 2019



Source: Global Connected Industries Cybersecurity Survey from Swedish software company Irdeto, https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/, Downloaded 2020-07-15

Health Care Data – Data Privacy

Health Care Data contains **most private information**:

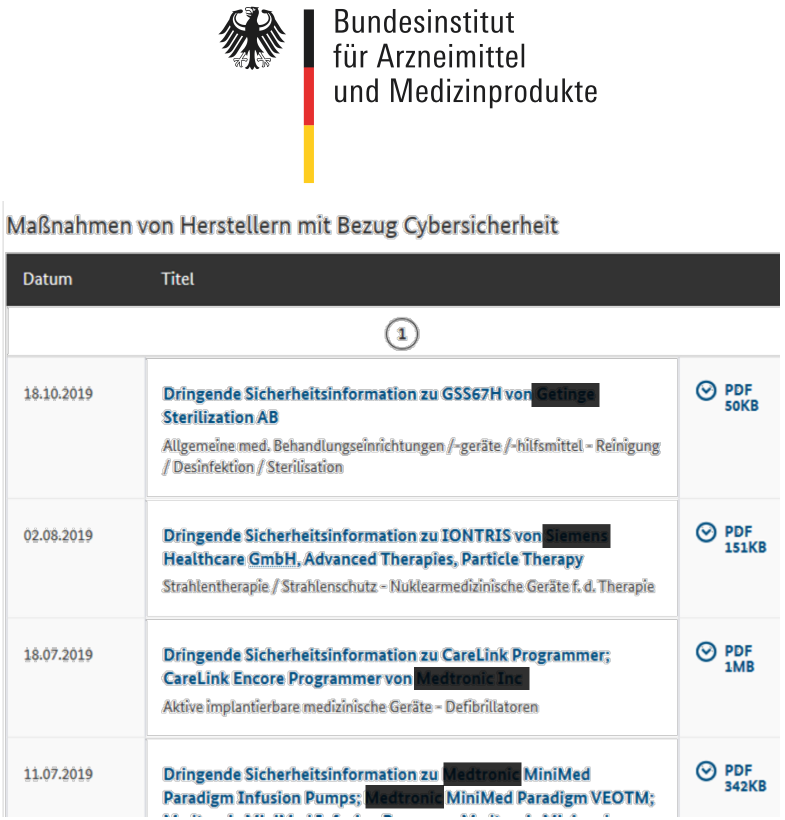
- Address, name, insurance information
- Medical conditions, diseases
- Drugs and therapies taken

2018: Singapore: Deliberate, **targeted** and well-planned **cyber attack** on SingHealth repeatedly **targeted PM Lee's personal particulars** and **information** on **medicine** that had been dispensed to him [11][12]

Medical device: **Radiation** therapy :

- Medical Product: **no** individual password
- Private internet router: with **individual** password

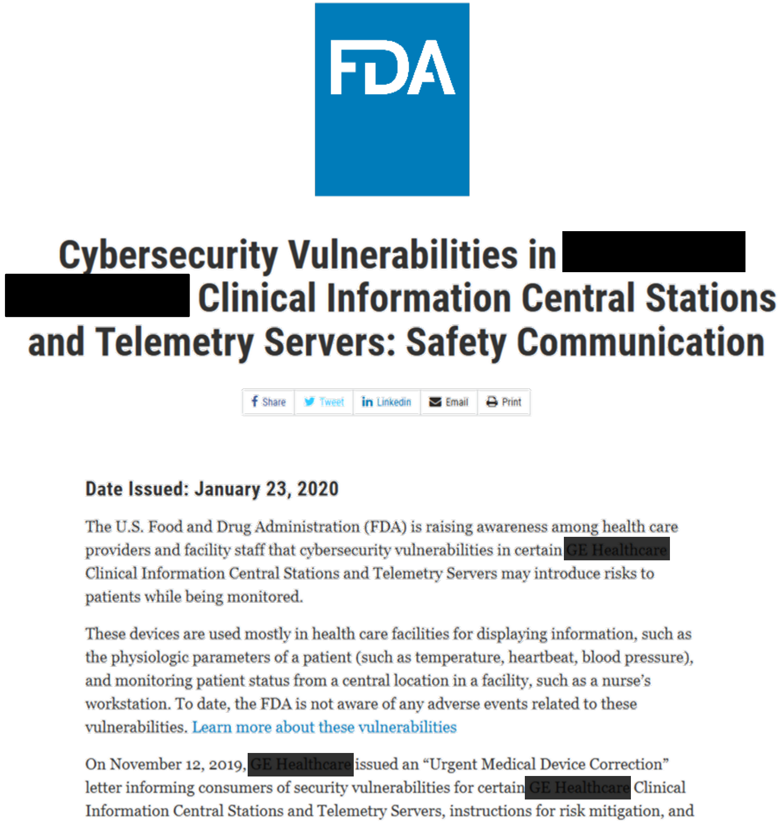
Reputational damage



Bundesinstitut
für Arzneimittel
und Medizinprodukte

Maßnahmen von Herstellern mit Bezug Cybersicherheit

Datum	Titel	
	1	
18.10.2019	**Dringende Sicherheitsinformation zu GSS67H von [redacted] Sterilization AB** Allgemeine med. Behandlungseinrichtungen /-geräte /-hilfsmittel - Reinigung / Desinfektion / Sterilisation	PDF 50KB
02.08.2019	**Dringende Sicherheitsinformation zu IONTRIS von [redacted] Healthcare GmbH, Advanced Therapies, Particle Therapy** Strahlentherapie / Strahlenschutz - Nuklearmedizinische Geräte f. d. Therapie	PDF 151KB
18.07.2019	**Dringende Sicherheitsinformation zu CareLink Programmer; CareLink Encore Programmer von [redacted]** Aktive implantierbare medizinische Geräte - Defibrillatoren	PDF 1MB
11.07.2019	**Dringende Sicherheitsinformation zu [redacted] MiniMed Paradigm Infusion Pumps; [redacted] MiniMed Paradigm VEOTM;**	PDF 342KB



Cybersecurity Vulnerabilities in [redacted] Clinical Information Central Stations and Telemetry Servers: Safety Communication

Date Issued: January 23, 2020

The U.S. Food and Drug Administration (FDA) is raising awareness among health care providers and facility staff that cybersecurity vulnerabilities in certain [redacted] Clinical Information Central Stations and Telemetry Servers may introduce risks to patients while being monitored.

These devices are used mostly in health care facilities for displaying information, such as the physiologic parameters of a patient (such as temperature, heartbeat, blood pressure), and monitoring patient status from a central location in a facility, such as a nurse's workstation. To date, the FDA is not aware of any adverse events related to these vulnerabilities. Learn more about these vulnerabilities

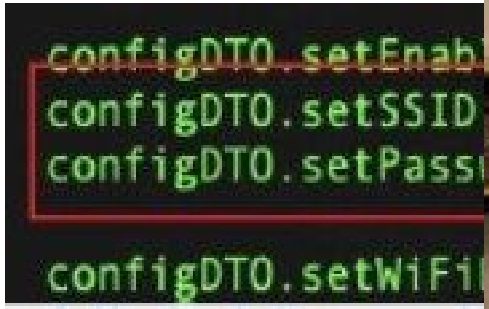
On November 12, 2019, [redacted] issued an "Urgent Medical Device Correction" letter informing consumers of security vulnerabilities for certain [redacted] Clinical Information Central Stations and Telemetry Servers, instructions for risk mitigation, and

Avoid being published here

Secure Solution & good coding principles

- MDCG publish new **guidance** to **fulfil** all relevant **cybersecurity requirements** in **Annex I of MDR** and **IVDR** (MDCG 2019-16)

- Section 3 specifies requirements on a **Secure** by **design** approach
  - Security Management
  - Specification of Security requirements
  - **Secure by design**
  - Secure Implementation
  - **Secure verification and validation**
  - Management of security-related issues
  - Security update management
  - **Security guidelines**

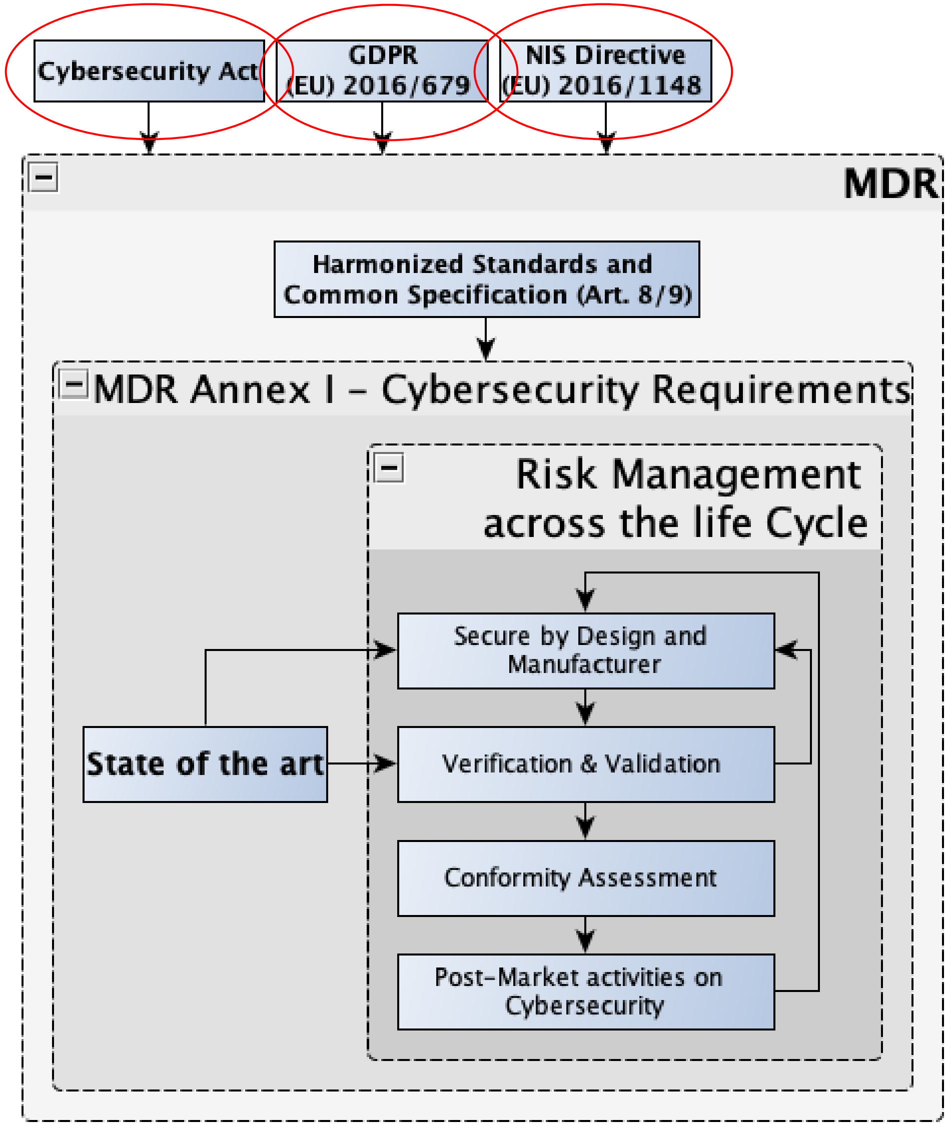


```
configDTO.setEnab
configDTO.setSSID
configDTO.setPass

configDTO.setWiFi
```

Secure Solution

- MDCG publish new **guidance** to **fulfil** all relevant **cybersecurity requirements** in **Annex I of MDR** and **IVDR** (MDCG 2019-16)
  - **NIS** directive to boost the overall cybersecurity with in the European Union
  - **GDPR** covering individuals persona data in EU
  - **Cybersecurity Act**: Certification Scheme


Cybersecurity Act
GDPR (EU) 2016/679
NIS Directive (EU) 2016/1148
MDR
Harmonized Standards and Common Specification (Art. 8/9)
MDR Annex I – Cybersecurity Requirements
Risk Management across the life Cycle
State of the art
Secure by Design and Manufacturer
Verification & Validation
Conformity Assessment
Post-Market activities on Cybersecurity

Challenges on the market and practical steps

- **Challenges on the market**
  - Higher *classifications* of Class I medical device software
  - Health apps are reimbursement by insurance companies (DE)
  - Missing harmonized standards
  - Increase interest of hackers on medical records and medical devices
- **Best Practice steps**
  - Consider: Cyber attacks don't just happen to large companies
  - Understand the treats
  - Adopt a risk based approach
  - Create a cyber risk management life cycle
  - Be able to detect an attack
  - Be prepared to react on incidences
  - Challenge and test regularly

Source: Universität Siegen

Summary

“As the level of threat is […] critical for medical devices, more suitable Cyber Security mechanisms will have to be developed in the future.”

“We need to do our utmost to protect critical healthcare systems […] and work towards improving the safety of the patients”

“Medical device manufacturers are responsible […] about identifying risks and hazards […] including […] cybersecurity.”

*Paris **call for trust and Security in cyberspace** in 2018 (French President Emmanuel Macron)*
***endorsed** by **64** countries*

Sign-up for **Healthcare and Medical Devices E-ssentials**, TÜV SÜD's complimentary newsletter about the latest regulations and standards, at: www.tuv-sud.com/e-ssentials

Dr.-Ing. Abtin Rad
Global Director Functional Safety, Software and Digitization

Medical & Health Services
TÜV SÜD Product Service Division

Abtin.Rad@tuev-sued.de

Francisco Navarro
Cyber Security Expert for Medical Devices

Medical & Health Services
TÜV SÜD Product Service Division

Francisco.Navarro@Tuev-Sued.de

Contact us:
www.tuv-sud.com
info@tuv-sud.com

Follow us on social media:

- instagram.com/tuvsud
- linkedin.com/company/tuv-sud
- twitter.com/tuvsud
- xing.com/companies/tuvsud
- youtube.com/tuvsud

Literature

[1] GLOBAL TRENDS TO 2030 CHALLENGES AND CHOICES FOR EUROPE, ISBN: 978-92-76-01898-8 • DOI: 10.2872/12232

[2] McAfee, Economic Impact of Cybercrime, Feb. 2018

[3] Reuters, Dowloaded 2020-05-11, https://www.reuters.com/article/us-hospira-fda-cybersecurity/fda-warns-of-security-flaw-in-hospira-infusion-pumps-idUSKCN0Q52GJ20150731

[4] REUTERS, J&J warns diabetic patients: Insulin pump vulnerable to hacking, Jim Finkle, OCTOBER 4

[5] EPRS | European Parliamentary Research Service, Author: Tania Lațici, Members' Research Service, PE 637.980 – July 2019

[6] Ghafur, S., Kristensen, S., Honeyford, K. et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digit. Med. 2, 98 (2019). https://doi.org/10.1038/s41746-019-0161-6

[7] World Economic Forum, The global Risk Report 2018, 13th Edition

[8] The Guardian, Dick Cheney feared assassination by shock to implanted heart defibrillator, Richard Luscombe, October 19, 2013

[9] https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and, downloaded: 2020-07-02

[10] 2018 Cost of a Data Breach Report, IBM, https://www.ibm.com/security/data-breach

[11] Tham, Irene (20 July 2018). "Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack". The Straits Times. Archived from the original on 22 August 2018. Retrieved 2 October 2018.

[12] Tham, Irene (20 July 2018). "SingHealth cyber attack: How it unfolded". The Straits Times. Archived from the original on 22 August 2018. Retrieved 2 October 2018

[13] https://www.medtechintelligence.com/column/medical-device-cybersecurity-in-the-age-of-iomt/ , Downloaded 2020-07-15

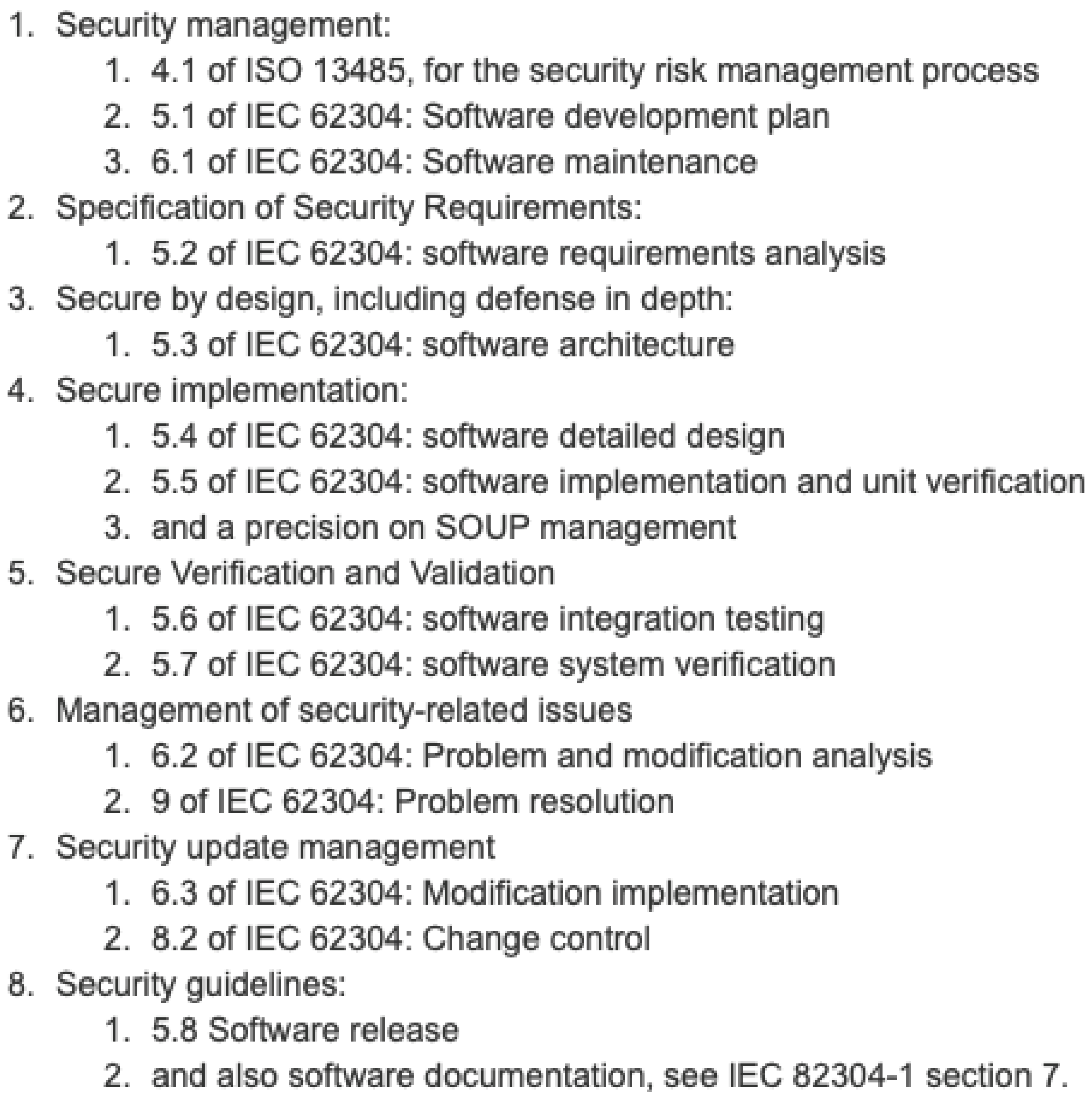
[14] Global Connected Industries Cybersecurity Survey from Swedish software company Irdeto, found in this page: https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/, Downloaded 2020-07-15

[15] https://www.mobihealthnews.com/content/johnson-johnson-warns-insulin-pump-users-possible-hacking-risk , picture downloaded 2020-07-16

[16] https://www.kaspersky.com/blog/drug-pump-security-bugs/8650/ , picture downloaded 2020-07-16

[17] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack, picture downloaded 2020-07-16

Additions



1. Security management:
    1. 4.1 of ISO 13485, for the security risk management process
    2. 5.1 of IEC 62304: Software development plan
    3. 6.1 of IEC 62304: Software maintenance
2. Specification of Security Requirements:
    1. 5.2 of IEC 62304: software requirements analysis
3. Secure by design, including defense in depth:
    1. 5.3 of IEC 62304: software architecture
4. Secure implementation:
    1. 5.4 of IEC 62304: software detailed design
    2. 5.5 of IEC 62304: software implementation and unit verification
    3. and a precision on SOUP management
5. Secure Verification and Validation
    1. 5.6 of IEC 62304: software integration testing
    2. 5.7 of IEC 62304: software system verification
6. Management of security-related issues
    1. 6.2 of IEC 62304: Problem and modification analysis
    2. 9 of IEC 62304: Problem resolution
7. Security update management
    1. 6.3 of IEC 62304: Modification implementation
    2. 8.2 of IEC 62304: Change control
8. Security guidelines:
    1. 5.8 Software release
    2. and also software documentation, see IEC 82304-1 section 7.

TIC COUNCIL

Follow us online

@TICCouncil

TIC Council

Wikipedia page:
Testing, inspection and certification

TIC-Council.org