

Cybersecurity of medical devices



Experience from PL PRES in the COUNCIL



When it comes to cybersecurity of medical devices, from my experience, I think they are



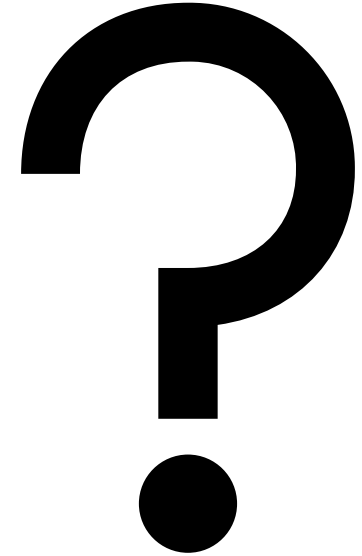
Where are cybersecurity requirements for medical devices contained?



Is cybersecurity checked by notified bodies in conformity assessment process?

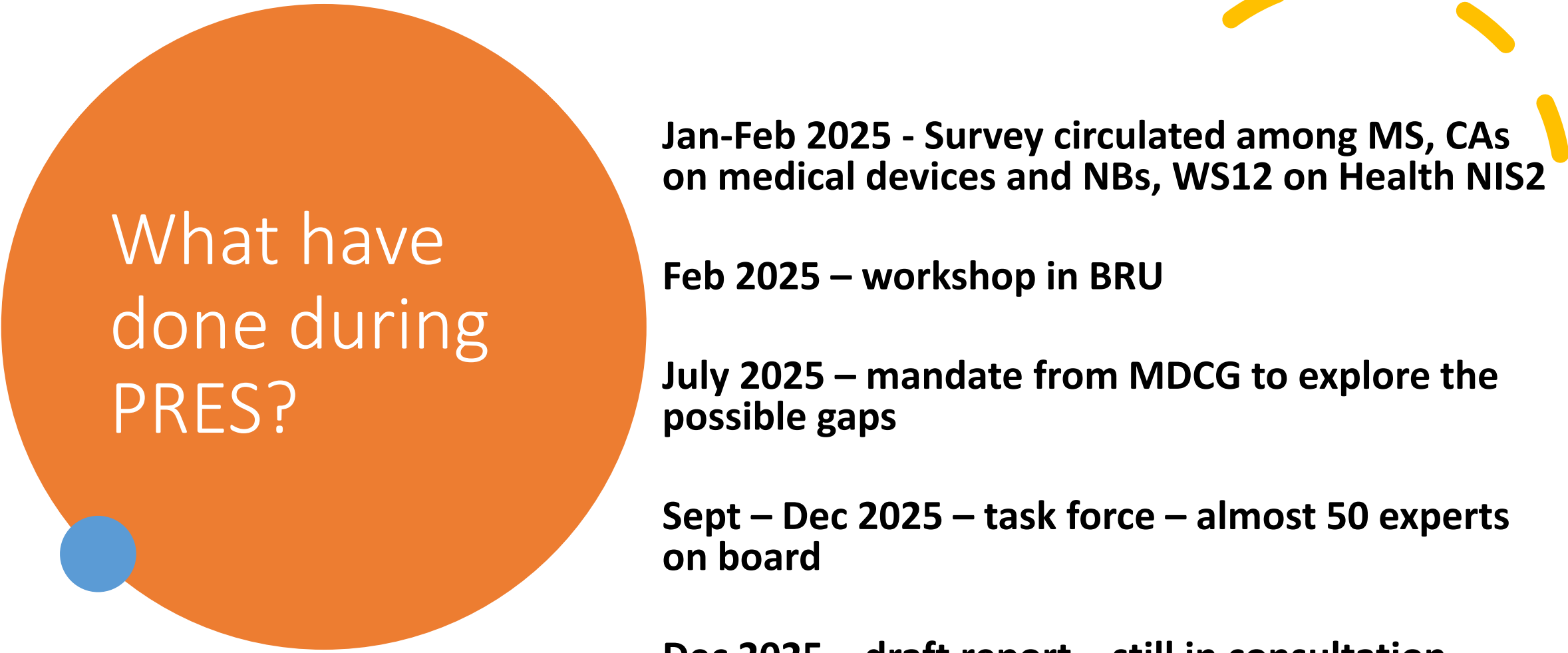
AGENDA

- Why did we start looking into this issue?
- What have done during PRES?
- What have we learnt during PRES and from the task force?
- What do we have in MDR/IVDR?
- What may help to figure out in details?
- What do we have in the CRA?
- Comparison MDR-CRA
- What do we have in EC Proposal?
- How to fine-tune the proposal?



Why did we start looking into this issue?

- Rising importance of compliance with NIS2 requirements - MDs important element in supply chain
 - Hospitals' concerns about securely connecting medical devices to hospital networks – are they secure?
 - Lack of clarity as to which cybersecurity requirements apply to medical devices, as they are excluded from the CRA
-do we have new candidate for European certification scheme???



What have done during PRES?

Jan-Feb 2025 - Survey circulated among MS, CAs on medical devices and NBs, WS12 on Health NIS2

Feb 2025 – workshop in BRU

July 2025 – mandate from MDCG to explore the possible gaps

Sept – Dec 2025 – task force – almost 50 experts on board

Dec 2025 – draft report – still in consultation...

What have we learnt during PRES and from the task force?

- No **direct** provisions in legal text (MDR)
- No major standards on cyber harmonized (IEC 81001-5-1 listed for cybersecurity as item 50, to be delivered by 27th of May 2028)
- Sometimes additional national requirements on cybersecurity in few MS
- MDCG 2019-16 Rev.1 "Guidance on Cybersecurity for medical devices" – an update needed
- 6 Horizon Europe projects ongoing on enhancing **medical device cybersecurity**
- Bottom – up efforts among NBs to standardize the assessment procedure
- Relatively low cybersecurity notifications to CAs
- Diversified approach between manufacturers:
 - to cyber incidents
 - to vulnerability handling

What do we have in MDR/IVDR?

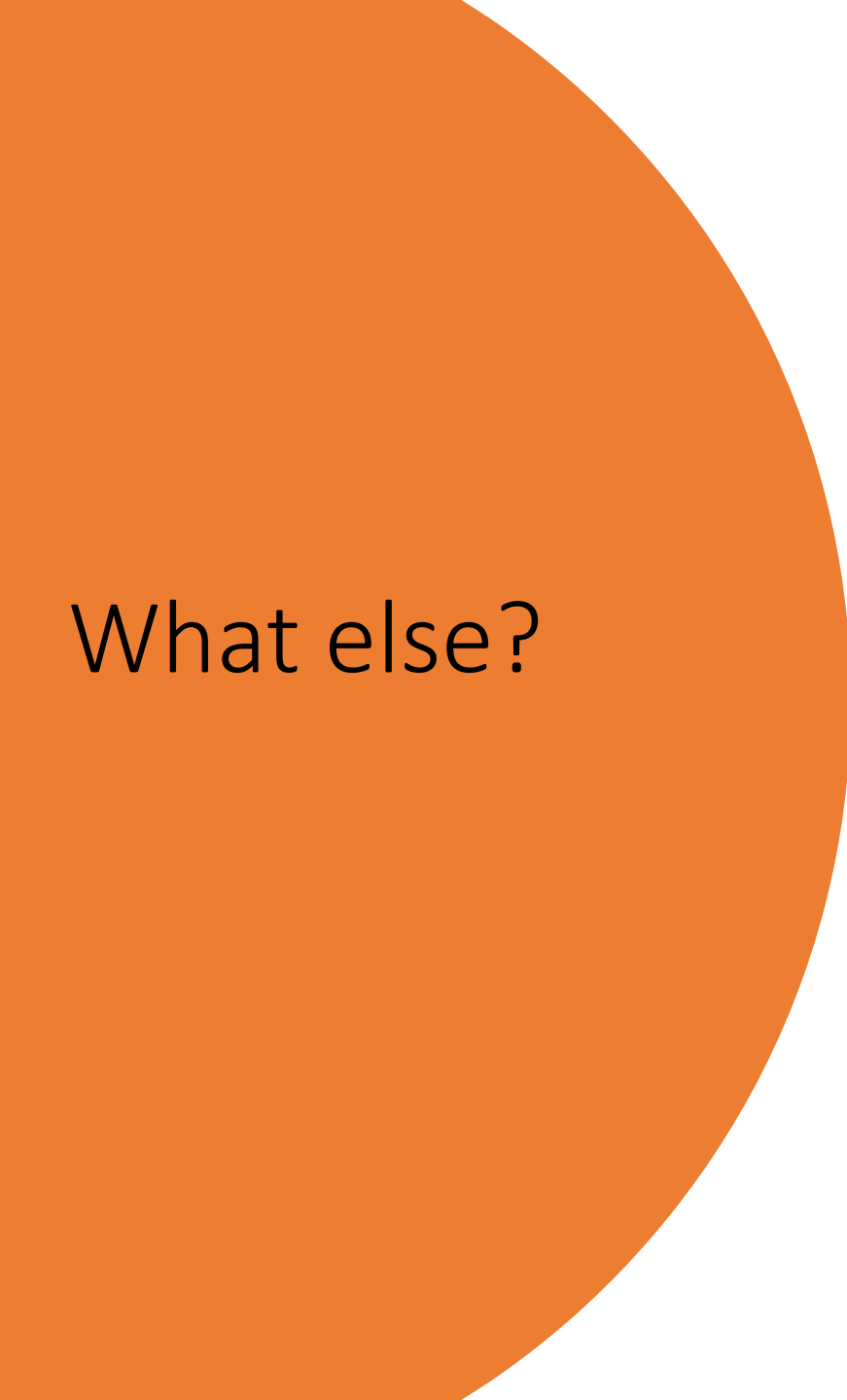
ANNEX I

14.2 (d) - requiring **devices to be designed and manufactured in such a way as to remove or reduce as far as possible 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.**

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 unauthorized access, necessary to run the software as intended.

A large orange circle is positioned on the left side of the slide, partially overlapping the text area.

What else?

- Several international standards including IEC TS 81001-5-1 (planned for 2028), IEC TR 60601-4-5, IEC 62304, ISO/IEC 29147:2018, ISO/IEC 30111:2019, 81001-2-2:2025 (in progress), **FDA Recognized Consensus Standard - IEEE 2621.2**
- CRA – is it state of the art ?

What do we
have in CRA?

CRA – Cyber Resilience Act 2024 - horizontal legislation focused on the cybersecurity and resilience of all products with digital elements; **MDs were excluded from the scope**

Annex I Essential cybersecurity requirements - 1,5 page

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

- (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
- (2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
 - (a) be made available on the market without known exploitable vulnerabilities;
 - (b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;
 - (c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;
 - (d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;
 - (e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;
 - (f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

Comparison MDR-CRA

1. **MDR addresses cybersecurity indirectly** via Annex I (e.g. 14.2 (d), 17.2-17.4 / IVDR 16.2-16.4) and relies on Interpretation of SOTA. CRA establishes explicit, prescriptive obligations (e.g. vulnerability handling, free updates, support period, SBOM, reporting d to ENISA / CSIRTs)
2. **CRA introduces requirements absent in MDR**, particularly relevant to connected medical devices. This concerns for example Software Bill of Materials (Annex I, Part II); Policy for coordinated vulnerability disclosure (Annex I, Part II); Publication of security support period end–date in instruction for use (Annex II) – which correspond to international standards on cybersecurity of MDs

What do we have in EC Proposal?

- **Cybersecurity per se mentioned in general safety and performance requirements in Annex I**

Section 17.4. is replaced by the following: *17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics, IT security measures and **cybersecurity**, including protection against unauthorized access, necessary to run the software as intended.'*

- **Mandatory Reporting of Actively Exploited Vulnerabilities - Article 87a**

Without prejudice to the reporting obligations regarding serious incidents and field safety corrective actions set out in Article 87, the manufacturer of a device shall report to the computer security incident response teams ('CSIRTs'), designated as coordinators of the Member States where a device has been made available, and to the European Union Agency for Cybersecurity (ENISA), either of the following:

(a) any actively exploited vulnerability as defined in Article 3, point (42), of Regulation (EU) 2024/2847 of the European Parliament and of the Council contained in the device;

(b) any severe incident as referred in Article 14(5) of Regulation (EU) 2024/2847 having an impact on the security of the device.

How to fine-tune the proposal?

What is needed?

1. **Essential cybersecurity requirements** similar to annex I in CRA added to MDR/IVDR to impose legally binding requirements and enhance legal clarity
2. Introducing **cybersecurity terminology to MDR/IVDR**
3. Clear **responsibility to patch vulnerabilities** on the risk based
4. **More transparency on the supply chain – SBOM**
5. **Clarifying and simplifying the reporting obligations.**



Magdalena Mycek
Urzędnik Służby Cywilnej Ministerstwo
Zdrowia



Magdalena Mycek, Counsellor, Ministry of Health, PL