NEMECYS: Improved guidance for cyber security of medical devices, in compliance with the Medical Device Regulation (MDR) and the In-Vitro Diagnostic Regulation (IVDR)

Karin Bernsmed, SINTEF (Norway)

ECSCI webinar, December 10th, 2024

NEMECYS
New Medical Cybersecurity and design Solutions

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union, by UK Research and Innovation (UKRI) and by the Swiss State Secretariat for Education, Research and Innovation (SERI).

About NEMECYS

HEU project on **cyber security of connected medical devices (CMD).**
12 partners, coordinated by SINTEF. Dates: 1st Jan 2023 – 31st December 2025.

Ambition:

- Investigate proportionate **cyber security risk-benefit** schemes
- Deliver **tools and toolboxes** for three stakeholder groups: manufacturers, integrators and operators (health service providers)
- Review relevant guidelines (MDCD 2019-16) and provide **recommendations** for improvement

Project results will be demonstrated in four representative case studies:

- Home dialysis, using a **bioimpedance sensor patch** from MODE Sensors (NO).
- Continuous monitoring of movement disorders, using a **wearable device** from PD Neurotechnology (UK).
- **IVD medical devices** for hospital point-of-care testing, operated at Ospedale San Raffaele SRL hospital (IT).
- **Mobile applications** (class IIb device) in hospitals and home environments, designed by Debiotec (CH) and used by Ribera Salud hospitals (ES).

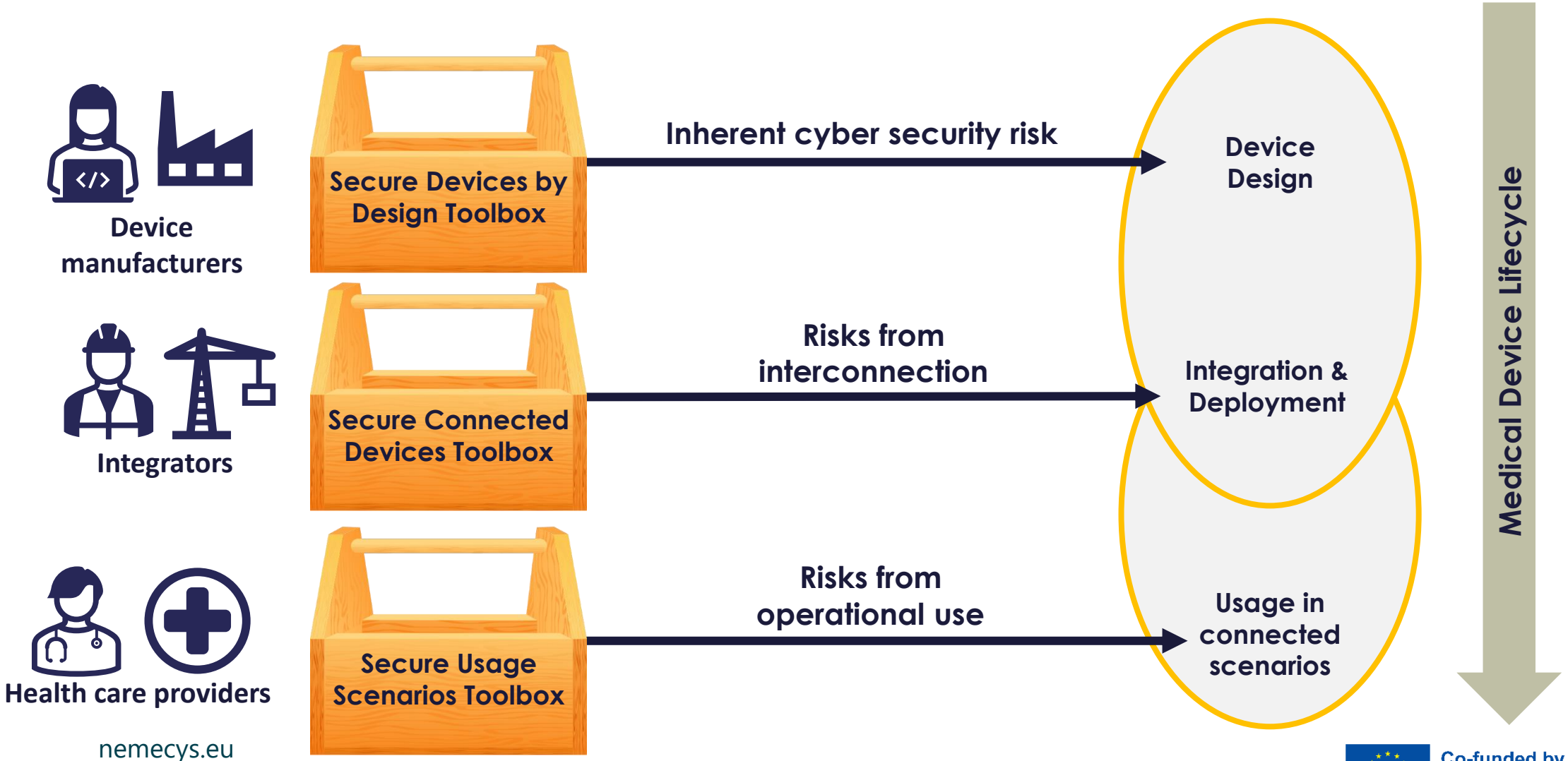
Together with research partners and technology providers: Univ. of Southampton (UK), IBM (IL), Athens Technology Center (EL), Univ. of Ioannia (EL) and Information Catalyst (UK and ES)

Questions? info@nemecys.eu

We welcome collaboration with all kinds of stakeholders from the healthcare domain!
http://nemecys.eu

Our stakeholders and toolboxes

NEMECYS
New Medical Cybersecurity and design Solutions



nemecys.eu

Co-funded by the European Union

Our case studies

NEMECYS
New Medical Cybersecurity and design Solutions

mode

Re:Balans

Home Dialysis

PDMonitor

Monitoring of Movement Disorders

pd neurotechnology
medical solutions

DEBIOTECH

SaMD

Mobile Phone Application

CGM

Monitoring of Diabetes

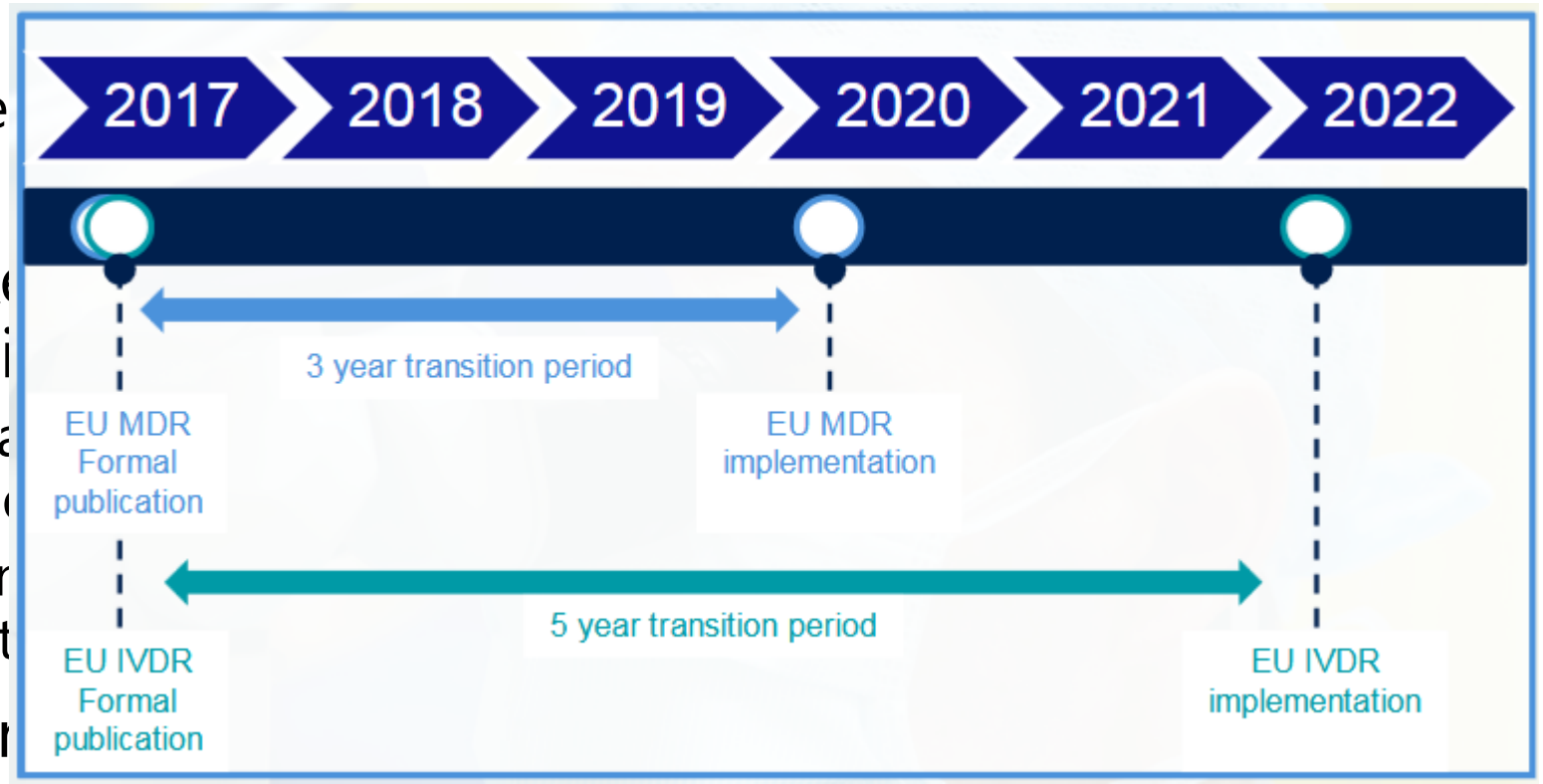
OSPEDALE SAN RAFFAELE

nemecys.eu

Co-funded by the European Union

What is the EU MDR and IVDR

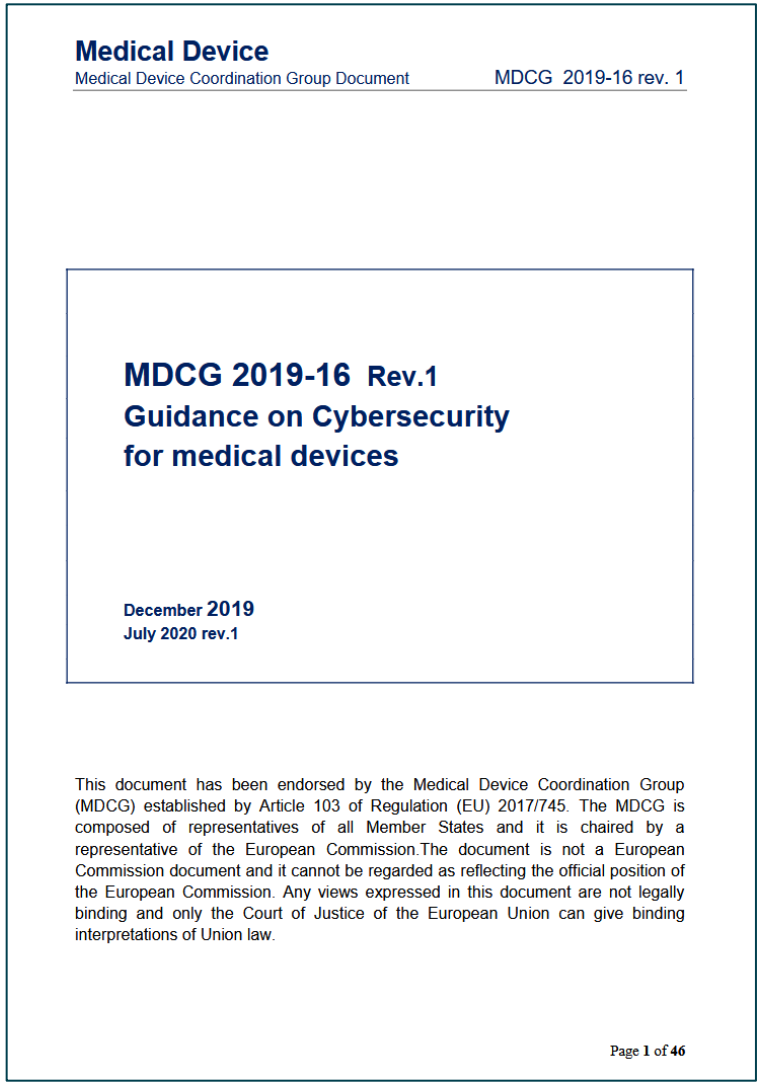
- The EU Medical Device Regulation (MDR) is a set of directives and rules that govern the production and distribution of medical devices in Europe
  - Applies to medical device
  - Covers "everything" from
- The EU In-Vitro Device R
  perform an *in vitro* functi
  - Applies to a vast list of dia
    specimens from within th
  - Examples include pregnar
    urinalysis kits, COVID-19 t
- Both these regulations e



Co-funded by
the European Union

The MDCG 2019-16 guidance

- Regulations can be hard to implement!
- The MDCG 2019-16 Medical Device Security Guidance is intended to assist practitioners in compliance with MDR and IVDR
- The Horizon Europe call "Enhancing cybersecurity of connected medical devices": HORIZON-HLTH-2022-IND-13-01 requested feedback to MDCG 2019-16:
  - Identify representative case studies
  - Evaluate the applicability of the guidance
  - Make recommendations



Medical Device
Medical Device Coordination Group Document MDCG 2019-16 rev. 1

MDCG 2019-16 Rev.1
Guidance on Cybersecurity for medical devices

December 2019
July 2020 rev.1

This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

Page 1 of 46

Co-funded by the European Union

Our feedback to the MDCG is a joint effort

NEMECYS
New Medical Cybersecurity and design Solutions

https://nemecys.eu/

Septon

https://septon-project.eu/

CYLCOMED

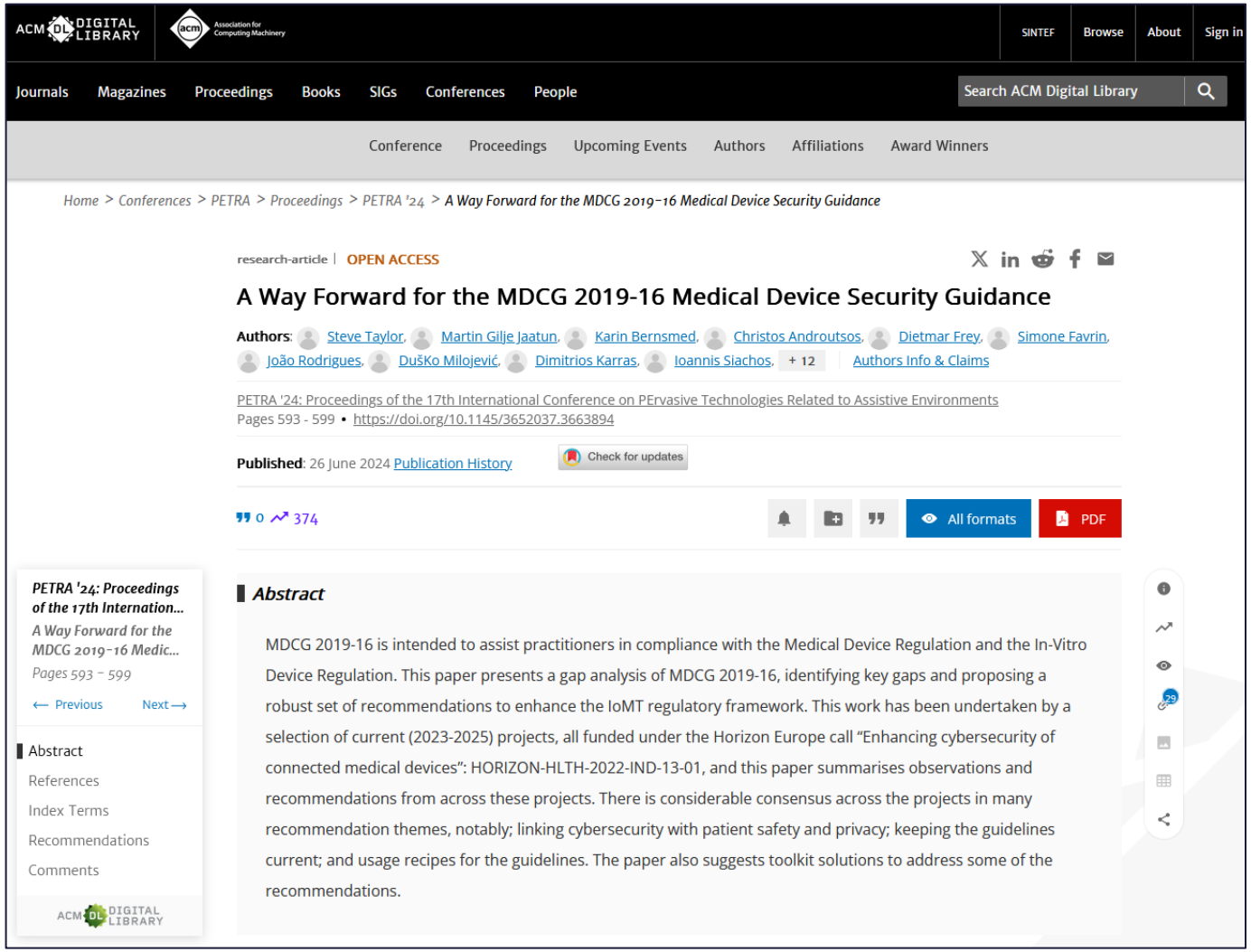
https://www.cylcomed.eu/

Enlightened trust in governance
EnTrust

https://entrust-project.eu/

MedSecurance
Advanced Security-for-safety Assurance for Medical IoT

https://www.medsecurance.org/



Co-funded by the European Union

Example of recommendations

- **Linking Cybersecurity Risks, Patient Safety & Privacy Risks (NEMECYS, CYLCOMED, MEDSECURANCE)**
  - It is not clear how cybersecurity techniques and privacy measures relate to patients' safety
  - Need to consider relationships between **cybersecurity consequences** (*"A security violation that results from a threat action"* (ISO/IEC 27001:2022)) and **patient harms** (*"injury or damage to the health of people, or damage to property or the environment"* (ISO 14971:2019))
  - A key integration point is via **data**, where a widely accepted set of risks is related to the CIA triad – Confidentiality, Integrity and Availability
    - E.g., compromises in the availability or integrity of MD sensor data can lead to late or inaccurate diagnosis, leading to potential patient harm

Co-funded by the European Union

Example of recommendations

- **Guidance on Cybersecurity Controls (NEMECYS)**
  - Absence of guidance in the MDCG on security-related controls with respect to device classes
    - Causes difficulties in identifying security control criteria for types of MD
  - Recommend that reference to **relevant cybersecurity risk management standards** such as ISO 27002 are recommended by MDCG

- **Balancing Different Types of Patient Risk (NEMECYS)**
  - Recommend that the MDCG provide guidance on resolution of conflicts
    - E.g. between privacy requirements, cybersecurity and medical needs
  - Advice on **methods to evaluate balances between conflicting needs** will enable decision maker to determine clear policy on acceptable balance between patient healthcare and privacy

Co-funded by the European Union

Example of recommendations

- **Keep MDCG 2019-16 Guidelines Current (NEMECYS, MEDSECURANCE)**
  - Recommended that MDCG guidelines are **periodically updated** with respect to evolving standards and state of the art
  - Also to keep pace with evolutions of MDR / IVDR

- **MD Lifecycle & Risk Assessment (NEMECYS)**
- Recommended that the MDCG guidelines map guidance to the **different stages of the whole MD lifecycle**:
  - Design and manufacturing, deployment in (many different) scenarios, operation of the device in those scenarios and decommissioning / disposal.
  - Different lifecycle stages of a medical device may give rise to differing priorities for cybersecurity or patient harm

Co-funded by the European Union

Conclusions

- The collaboration with our five HEU sibling projects has been a great success!
- Together, we have suggested 12 recommendations towards improving the guidance represented in MDCG 2019-16
- Considerable consensus across the projects in many recommendation themes, notably:
  - linking cybersecurity with patient safety and privacy;
  - keeping the guidelines current; and
  - usage recipes for the guidelines.
- All projects are at their halfway point, and subsequent papers / policy briefs will describe further recommendations to the MDCG 2019-16 guidelines as appropriate

Co-funded by the European Union

Thank you for listening!

NEMECYS
New Medical Cybersecurity and design Solutions

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union, by UK Research and Innovation (UKRI) and by the Swiss State Secretariat for Education, Research and Innovation (SERI).