# NEMECYS

New Medical Cybersecurity and design Solutions

# NEw MEdical CYbersecurity assessment and design Solutions

## What is NEMECYS?

Personalised healthcare services are the future, and connected medical devices will play a critical role. The NEMECYS project is dedicated to developing innovative cybersecurity assessment techniques and tools that promote security-by-design for connected medical devices.

## NEMECYS Objectives

The NEMECYS project aims to:

**Review Medical Device (MD) guidelines**

to provide recommendations for improvement. Using four case studies, experts will identify gaps, suggest solutions, and establish best practices for Connected Medical Devices (CMDs).

**Develop proportionate risk-benefit schemes**

by enhancing state-of-the-art research and delivering cybersecurity risk assessment tools tailored to CMD environments.

**Create targeted tools and toolboxes**

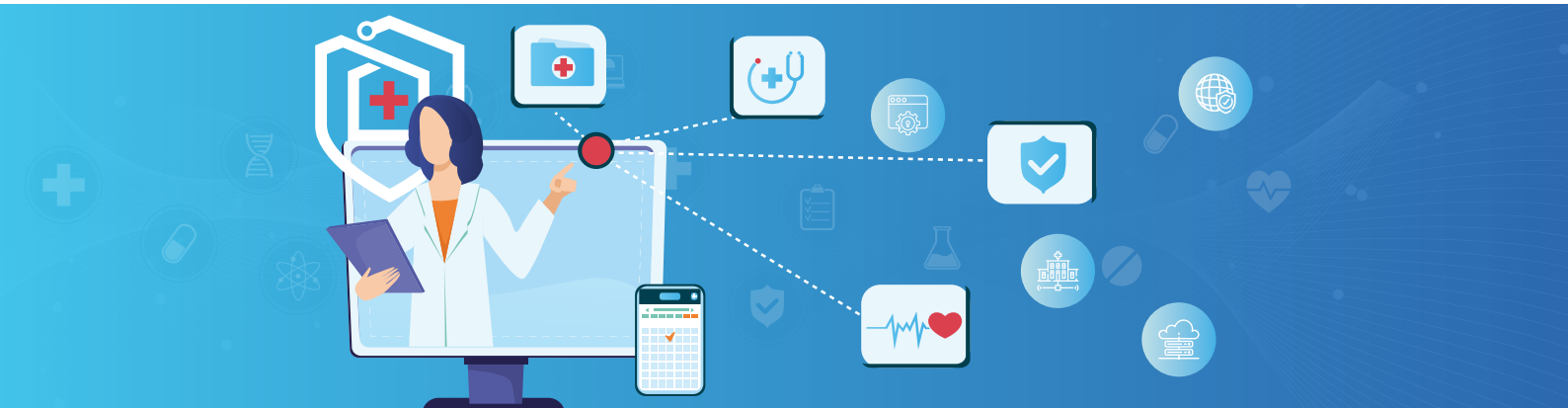
for three user groups involved in CMD lifecycles: **CMD Manufacturers**, **CMD System Integrators** and **CMD Operators** such as hospitals or care providers.

## What to expect from NEMECYS?

**NEMECYS will deliver:**

- **Tool-supported methods** to facilitate semi-automatic CMD compliance.
- **Risk/benefit analysis tools** for AI/ML-driven medical software.
- **Data privacy solutions** for medical devices using AI/ML.
- **Secure integration methods** for CMDs in multi-stakeholder environments.
- **CMD management and vulnerability detection tools**.

All NEMECYS tools and methods will be validated through **four real-world case studies** addressing connected medical device scenarios. Those are “Bioimpedance measurement patch”, “Wearable medical device for continuous monitoring of movement disorders”, “Mobile application intended for therapy support or diagnosis” and “hospital based point-of-care testing”.



## NEMECYS Use Cases

NEMECYS has defined those **distinct use cases** to:

Serve as a foundation for **requirements gathering** in risk-benefit analysis and cybersecurity tool development.

Identify **gaps in current cybersecurity guidelines** and best practices.

**Validate NEMECYS risk-benefit analysis tools** and cybersecurity toolboxes during later phases of the project.

## NEMECYS Tools

NEMECYS offers a comprehensive suite of tools designed to improve cybersecurity in connected medical devices. These tools focus on enhancing privacy protection, streamlining risk assessment processes, strengthening secure software development practices, and ensuring effective vulnerability detection and management. By addressing each phase of a medical device's lifecycle, NEMECYS tools support manufacturers, system integrators, and healthcare providers in implementing security-by-design principles and ensuring compliance with regulatory standards.

**Toolboxes**

## NEMECYS Target Groups

**The NEMECYS project's outcomes will benefit:**

- **Healthcare Industry** stakeholders such as CMD manufacturers, suppliers, integrators, healthcare providers, and operators.
- **Regulatory Bodies** like the MDCG, along with advisory institutions.
- **Patients and Society** by enhancing the security and trustworthiness of connected medical devices.
- **The Scientific Community** and **Cybersecurity Experts** through cutting-edge research and technological advancements.

## Stay Connected with NEMECYS

For more information about the NEMECYS project, visit our website or follow us on social media to stay informed about our progress and outcomes.

**www.nemecys.eu**

**@NEMECYS_eu**

**nemecys-horizon-eu-project**

SINTEF

mode

IBM

ATC
ATHENS TECHNOLOGY CENTER

ribera

I.R.C.C.S. Ospedale San Raffaele
Gruppo San Donato

Med&Lab

ICE Information Catalyst

University of Southampton

pd neurotechnology
medical solutions

DEBIOTECH

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research and Innovation (SERI). The information and views set out in this publication are those of the author(s) only and do not necessarily reflect hose of the European Union, HADEA, UKRI or SERI. Neither the European Union nor the granting authorities can be held responsible for them.