COCIR and MedTech Europe Vision for Strengthening Cybersecurity in Europe's Future Healthcare Systems

Introduction

The healthcare sector in the European Union is at a critical juncture, where the integration of digital health technologies presents a unique opportunity to address some of the most pressing challenges facing health systems today. These challenges include staff shortages, financial constraints, and the growing need for personalised healthcare. However, with these opportunities come significant risks, particularly in the realm of cybersecurity. As EU healthcare providers, especially hospitals, become more digitally integrated, they increasingly face security threats, such as ransomware attacks and hacks by geopolitical actors. These cyberattacks can disrupt essential healthcare services and lead to the theft of sensitive patient data, posing a serious threat to the safety and trustworthiness of European Health Systems.

Recognising these challenges, President von der Leyen announced that the European Commission will publish a proposal for a European action plan on the cybersecurity of hospitals and healthcare providers within the first 100 days of the mandate. COCIR and MedTech Europe welcome this initiative and sees it as a crucial step toward securing Europe's healthcare systems for the future. This action plan aligns with COCIR and MedTech Europe's shared vision to enhance the resilience of healthcare infrastructures through comprehensive cybersecurity measures, ensuring that the benefits of digital health technologies can be fully realised without compromising patient safety or data integrity.

Current Legislative Framework

The European Union has begun to recognise these challenges through initiatives such as the NIS2 Directive and the requirements under the Medical Devices Regulation (MDR), the *In Vitro* Diagnostic Medical Devices Regulation (IVDR), and the changes proposed within the recent European Parliament resolution. These legislative measures are crucial steps in the right direction, as they establish a framework for enhancing the cybersecurity of healthcare systems across the EU. However, legislation alone is not sufficient to address the growing cybersecurity threats. Effective implementation of these legislations requires substantial support, including investments in infrastructure, software, and human resources.

Support Beyond Legislation

To achieve the objectives set out in the NIS2 Directive and other relevant legislation, it is essential to provide support that goes beyond the mere enactment of laws. This support should include investments in upgrading outdated infrastructure and software, the deployment of innovative and state-of-the-art cloud services and Software as a Service (SaaS) models, and the development the skills and expertise of healthcare and hospital personnel. We welcome the European Commission's new action plan aimed at increasing the security of European health systems, as it is a critical prerequisite for ensuring safe, high-quality healthcare across the EU.

Recommended Actions

To effectively implement the European action plan for cybersecurity in hospitals and healthcare providers, we recommend the following actions:

1. **Increase Capacity and Expertise in Healthcare**
    - Develop and implement a dedicated cybersecurity skills development and up-skilling program for health authorities, hospitals, and healthcare providers. This program should focus on enhancing cybersecurity expertise and building capacity within the healthcare sector to respond to and mitigate cyber threats effectively.

2. **Addressing the Risk of Obsolete Medical Technologies and Software**
    - Establish dedicated funding programs to upgrade or replace outdated software and hardware in the healthcare environment. The existence of a very old installed base of medical technologies and software may present cybersecurity risks that must be addressed. In this regard, medical technology manufacturers are prepared to mitigate risks owing to legacy devices as far as possible, within the existing MDR/IVDR frameworks.

3. **Awareness Raising and Stakeholder Engagement**
    - Launch an awareness-raising campaign for the NIS2 Directive in healthcare, including the organisation of stakeholder webinars at national and regional levels. These webinars should facilitate coordination, collaboration, and the exchange of best practices among healthcare providers, health authorities, and technology providers, as well as helping entities understand what aspects of their organisation are specifically in scope.

4. **Guidelines for Implementation of the NIS2 Directive in Healthcare**
    - Develop and disseminate dedicated guidelines for the implementation of the NIS2 Directive within the healthcare sector. These guidelines should focus on clarifying the requirements between different applicable legislations, particularly the MDR and IVDR, but also the EHDS and Cyber Resilience Act (for health software that does not qualify as Medical Device or IVD). The guidelines should emphasise the importance of shared responsibility and communication between healthcare delivery organisations and health technology providers. Additionally, promote the adoption of MDS2 (Manufacturer Disclosure Statement for Medical Device Security) as a best practice tool for effective communication regarding cybersecurity risks and mitigations. These guidelines should also drive harmonisation across Europe to improve access to new and more secure healthcare products and services.

5. **A Cloud Ecosystem that Underpins the Cybersecurity of European Healthcare**
    - A focus on state-of-the-art cybersecurity and innovative offering within the European cloud ecosystem, rather than erecting barriers based solely on political perceptions. In doing so, the European healthcare system will continue to benefit from cutting-edge cybersecurity of cloud service offerings.

6. **Embedding Cybersecurity in Healthcare Procurement**
    - Update the guidelines for embedding cybersecurity considerations in healthcare procurement[1], following the latest legislative and technological developments. These guidelines should ensure that cybersecurity is a fundamental criterion in the selection of medical technologies, software, and other healthcare technologies, while ensuring practical cybersecurity protections for the industry, also in view of the upcoming revision of the Public Procurement Directive.

Conclusion

COCIR and MedTech Europe are committed to working closely with the European Commission, ENISA, member states, and all relevant stakeholders to ensure the successful implementation of this vital action plan. The announcement by President von der Leyen to propose a European action plan on the cybersecurity of hospitals and healthcare providers within the first 100 days of the mandate underscores the urgency and importance of this issue. We believe that by taking the recommended actions outlined in this statement, we can significantly enhance the security of European health systems, safeguard patient data, and ensure the delivery of safe and high-quality healthcare services across the EU.

This collective effort will not only protect healthcare providers from emerging cyber threats but will also foster innovation and trust in digital health technologies. COCIR and MedTech Europe are fully aligned with the vision for a secure, resilient, and future-proof healthcare infrastructure in Europe, and we look forward to contributing to the success of this initiative.

About us:

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries. Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium). COCIR is unique as it brings together the healthcare, IT and telecommunications industries.

For more information, please contact:

Annabel Seebohm, COCIR Secretary General

Philipp Goedecker, COCIR Digital Health Senior Manager

[1] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

For more information, please contact:

Alexander Olbrechts, Director Digital Health

Benjamin Meany, Manager Digital, Software and AI Regulation