Proposal for a Regulation on horizontal cybersecurity requirements for digital products and ancillary services (Cyber Resilience Act)

MedTech Europe response to the European Commission Call for Evidence for an Impact Assessment

25 May 2022

Digital health and care technologies can innovate and improve access to care and quality of care and make healthcare delivery more efficient. Providing secure devices and services and keeping users and patients safe and protected is a core goal of the medical technology industry. Thus, the medical technology industry invests significant resources in guaranteeing baseline cybersecurity requirements for all products and services, including the data they produce.

Given the particularly sensitive nature of health data, the medical technology industry is keen on advancing the conversation around cybersecurity, and we welcome the opportunity to contribute to the European Commission's call for evidence for an Impact Assessment on the Cyber Resilience Act.

Medical technologies are designed to be safe and secure

The medical technology industry's cornerstone legislation, the Medical Devices Regulation and the *In Vitro* Diagnostic Medical Devices Regulation ("MDR" and "IVDR"), updated to the latest regulatory standards in 2017, afford a high level of protections for device users as a result of the manufacturing, design, and development processes of medical technologies. As "vendors", medical technology manufacturers and software developers continue to be tightly regulated under this legal framework.

The MDR/IVDR provide for a broad set of requirements on medical technologies, including for medical device software, accessing the EU Internal Market. This includes the design process (concerning risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts). In addition, MDR/IVDR requirements also cover the process of conformity assessment and the obtaining of a CE-Marking, the use of database registration, the notification to Notified Bodies, during continued incident reporting following market deployment, within the Quality Management System. It also relates to Post-Market Surveillance, as well as continued vigilance for instances of malfunctioning of the medical technology. Provisions on information security are also included, specifically for MD/IVD software, which ensure the cybersecurity of products reaching the market, and thus the cybersecurity of devices reaching/serving users and patients. Furthermore, medical devices integrating software or medical device software itself is required to 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"[1].Thus, medical technologies are designed in full consideration of the cybersecurity of the device.

Avoid misalignments and divergences from sectoral legislation

The MDR/IVDR ensure that medical technologies afford innovative safety and security to users and patients. It is therefore critical that any horizontal regulatory measures in the form of the European Commission's upcoming Cyber Resilience Act, duly consider existing protections and requirements enshrined in sectoral legislation.

It is essential that any additional requirements on medical technologies consider existing sectoral legislation. For example, requirements concerning software design are currently well accounted for in the pre-market deployment process of medical devices and *in vitro* diagnostics, enshrined within the MDR/IVDR. Misalignment between the forthcoming Cyber Resilience Act and the sectoral MDR/IVDR would likely result in legal uncertainty for manufacturers and developers, particularly in how sectoral requirements would interact with new horizontal requirements. Fragmentation as a result of regulatory misalignment and inconsistencies could produce unnecessary burdens on manufacturers of medical technology, especially if they are small or medium-sized enterprises. This, in turn could have a negative effect on the healthcare system, with the risk of inhibiting manufacturers from placing innovative medical technology on the EU Internal Market. A lack of legal certainty would also likely impact on the overall resilience of the digital ecosystem.

Cybersecurity is a shared responsibility

The medical technology industry is ready to play its part in ensuring the resilience of the digital health ecosystem. While we commend the European Commission's upcoming Cyber Resilience Act and support harmonised legislation, there are additional steps, including non-legislative measures, that lawmakers can employ to address the critical challenges of an expanding cybersecurity threat landscape.

The current complexities of the cybersecurity landscape show us that it is not only vulnerabilities of connected devices that should be addressed. To face these challenges directly, MedTech Europe strongly advocates for public action, for example in the form of investment, to address the overall cybersecurity gap in public healthcare institutions, MedTech Europe recommends some general actions, including:

- development of organisation-wide and specific cybersecurity strategies;
- ringfencing of funding dedicated to the training of information security and cybersecurity personnel;

[1] Medical Devices Regulation, Annex I on General Performance and Safety Requirements, Chapter I, 17.2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

- wider investments in cybersecurity training and skilling, both at organisational level but also within formal education.

MedTech Europe also urges the European Commission to duly consider work underway at the level of the International Medical Device Regulators Forum (IMDRF)[2], and the Medical Devices Coordination Group (MDCG)[3], in particular existing cybersecurity guidance.

The medical technology industry is prepared to support initiatives aimed at reinforcing the overall resilience of the European and global digital health ecosystem.

About MedTech Europe

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: Michael Strübin, Director Digital Health: m.strubin@medtecheurope.org

[2] Working Group on the Medical Devices Cybersecurity Guide

[3] MDCG 2019-16 - Guidance on Cybersecurity for medical devices