Cybersecurity requirements according to Medical Devices Regulations MDR 2017/745

In an increasingly interconnected world, thanks to technological advances in the design of electronic devices, cybersecurity plays a central role in protecting them from attacks that would undermine their reliability.

How can we define the concept of Cybersecurity?

Cybersecurity is defined by CISA (America's Cyber Defense Agency) as "The art of protecting networks, devices, and information from unauthorized access or criminal use, and the practice of ensuring the confidentiality, integrity, and availability of information" [1]. Cybersecurity, therefore, is a set of practices that ensure the defense of electronic devices, which are characterized by the possibility of being implemented in different application fields.

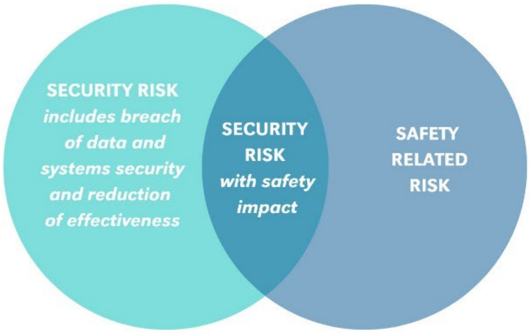
Specifically, in the medtech area, the specifications relating to cybersecurity are listed in Annex I of the Medical Devices Regulations (MDR 2017/745) [2]: these define the minimum security requirements to be met both during the design and marketing of medical devices, including IVDs ("In Vitro Diagnostic" medical devices).

What are the key concepts when talking about Cybersecurity for Medical Devices?

IT security for medical devices refers primarily to the following concepts:

- <u>Confidentiality</u> of information, both at rest and in transit;
- <u>Integrity</u>, to guarantee the authenticity and accuracy of data;
- <u>Availability</u> of processes, devices, data, and connected systems.

These three key concepts are summarized by the acronym CIA: "Confidentiality, Integrity, and Availability." Manufacturers are therefore responsible for developing medical devices in accordance with the state of the art, taking into account the principle of risk reduction in the field of information security. Moreover, not all risks related to the security of IT systems impact only the technological aspect of these devices, but could also have negative safety implications. It is therefore vital to implement risk reduction measures through cybersecurity practices throughout the life cycle of the medical device, through an iterative process that requires regular system updates [3].



Cybersecurity measures may cause safety impacts, according to MDCG 2019-16 [3]

To clarify the concept of security risk, consider the following example: a ventilator for assisted breathing is attacked by malware through physical access to the device via a USB interface. The attack results in the device failing to function, which can compromise patient safety during treatment. Protecting access ports to the medical device is therefore vital, as not only does a lack of protection pose a risk to the device itself, but also to its proper functioning and, therefore, the patient's health during its intended use. Cybersecurity techniques are designed to protect the device from unwanted access, ensuring its functionality.

Are there any working groups focused on the harmonization of medical devices Cybersecurity approaches?

The harmonization of the approach to medical device cybersecurity is the goal of an international working group of the International Medical Device Regulators Forum (IMDRF), which is drafting the Medical Device Cybersecurity Guide [4]. This document clarifies the fundamental aspects relating to device security, providing guidance for the design of devices by taking into account innovation, performance and safety.

In conclusion, minimum cybersecurity requirements must be considered throughout the medical device's life cycle, from design to distribution and maintenance, to ensure maximum performance and protect the health and safety of the various stakeholders involved.

References:

[1] “What is Cybersecurity?”, www.cisa.gov

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council

[3] MDCG 2019-16 Rev.1, Guidance on Cybersecurity for medical devices

[4] Medical Device Cybersecurity Guide, www.imdrf.org

Keywords: Cybersecurity, Medical Devices, MDR 2017/745, MDCG 2019-16, safety, security

Author: Gaia Di Federico, R&D Electronic Engineer