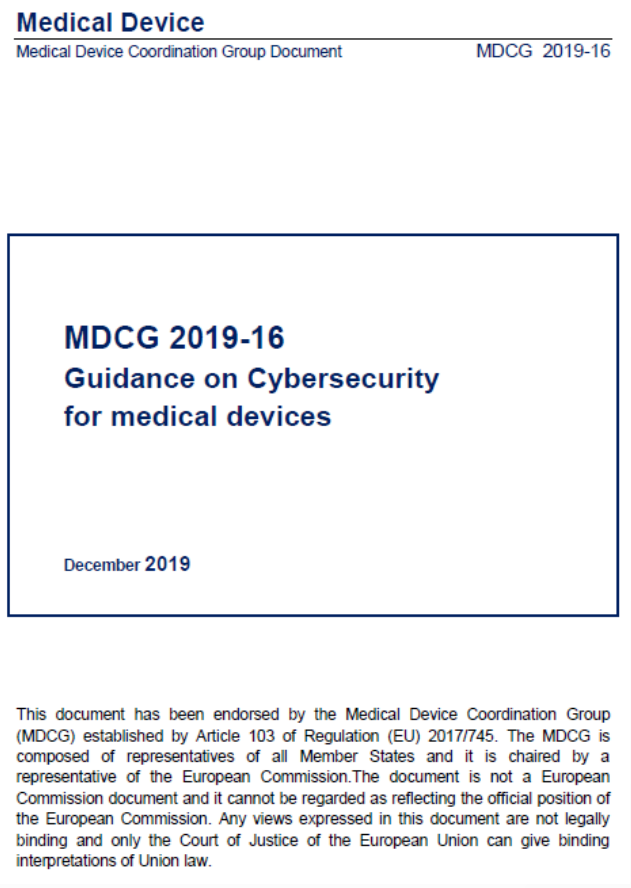
MedTech Europe
from diagnosis to cure

Cybersecurity:
It is a shared responsibility

MedTech Europe pitch at the eHAction workshop
“Common governance principals for the re-use of health data”
23-25 June 2020

Cybersecurity in the eHealth and Digital Ecosystem



Medical Device
Medical Device Coordination Group Document MDCG 2019-16

MDCG 2019-16
Guidance on Cybersecurity for medical devices

December **2019**

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.

ENISA's Executive Director, Juhan Lepassaar, stated (31st Oct, 2019: "***Cybersecurity remains a joint responsibility….***"

The sensitive and private nature of patient data means cyber security is a particularly important issue in the medical device industry

Smart technologies have made healthcare a more interconnected ecosystem – but may have done so at the expense of genuinely secure cyber defences (Credit: Arxan Technologies)

Healthcare providers are increasingly moving towards a "never trust, always verify" approach, also known as the "zero trust" security model, in order to protect networks and devices against an expanding threat landscape.

Cybersecurity in eHealth (including AI/ML) & Lack of Trust

eHealth agencies need to work with cybersecurity agencies to create guidances (no new regulation) taking into account that Medical Technologies:

- Long history of continuous evolution, with new types of technology being incorporated into MD's, with developed specific new standards and requirements to properly analyze security risks and evaluate safety.
- The advent of increased use of AI in MD is not out of the ordinary, in terms of both the need and the capability of regulators to analyze the risks and develop the guidances and requirements to properly evaluate the risks and ensure patient safety.
- Guidances need to address the increasing risk of cyberattacks by planning and deploying intelligent medical devices, to increase the users' trust.

Heavily regulated sector

Several EU legislative frameworks have introduced requirements for the security of connected health technologies:

- Medical Devices Regulation (MDR) & In Vitro Diagnostics Regulation (IVDR)
- Directive on Security of Network and Information Systems (NIS Directive)
- General Data Protection Regulation (GDPR)
- Cybersecurity Act

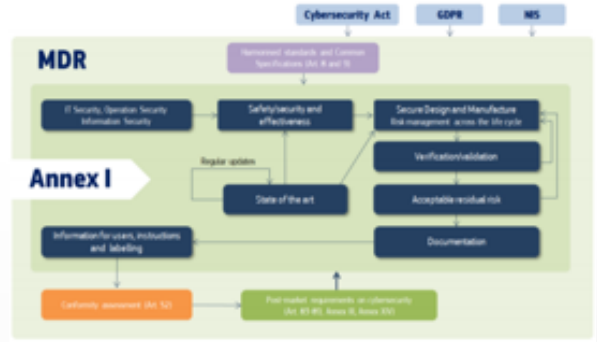


Figure 2: Cybersecurity requirements in the MDR; the application of other relevant EU legislations, such as Cybersecurity Act, GDPR and NIS is discussed in more detail in Chapter 7

MedTech Europe

Take into account:

- IMDR Principles and Practices for Medical Device Cybersecurity
- EC's MDCG 2019-16 Guidance on Cybersecurity for medical devices
- International Standards: ISO/IEC; CEN/CENELEC; ETSI; etc

MedTech Europe
from diagnosis to cure

Martha De Cunha Maluf-Burgman, vice Chair Digital Health Committee, MedTech Europe

decunm1@medtronic.com

www.medtecheurope.org

MedTech Europe
from diagnosis to cure