1. Introduction

1.1. Background

The two new Regulations on medical devices 745/2017 (MDR) and 746/2017 (IVDR) (hereafter called the Medical Devices Regulations) have been adopted and entered into force on 25 May 2017. The two Regulations, which are to replace three EU Directives[1], apply progressively until May 2020 for medical devices and May 2022 for *in vitro* diagnostic medical devices.

Among the many novelties introduced, the two Regulations enhance the focus of legislators on ensuring that devices placed on the EU market are fit for the new technological challenges linked to cybersecurity risks. In this respect, the new texts lay down certain new essential safety requirements for all medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. They require manufacturers to develop and manufacture their products in accordance with the state of the art taking into account the principles of risk management, including information security, as well as to set out minimum requirements concerning IT security measures, including protection against unauthorised access.

1.2. Objectives

The primary purpose of this document is to provide manufacturers with guidance on how to fulfil all the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity. However, and in light of the complexity of medical device supply chains and the role played by different operators in ensuring that devices are protected against unauthorised access and possible cyber threats, additional considerations concerning expectations from actors other than manufacturers are provided. In addition, a description of other EU and global pieces of legislation and guidance that are relevant to the domain of cybersecurity for medical devices has been provided in an Annex.

1.3. Cybersecurity Requirements included in Annex I of the Medical Devices Regulations

Cybersecurity requirements listed in Annex I of the Medical Devices Regulations, deal with both pre-market and post-market aspects. These requirements, and their interconnection, are illustrated in Figure 1 and are elaborated in Chapter 2 with the aim to provide a basis for the development of recommendations and guidance for medical device manufacturers (Chapters 3-6 of this document).

[1] Medical Device Directive (93/42/EEC), Directive on active implantable medical devices (90/385/EEC) and Directive on in vitro diagnostic medical devices (98/79/EC)

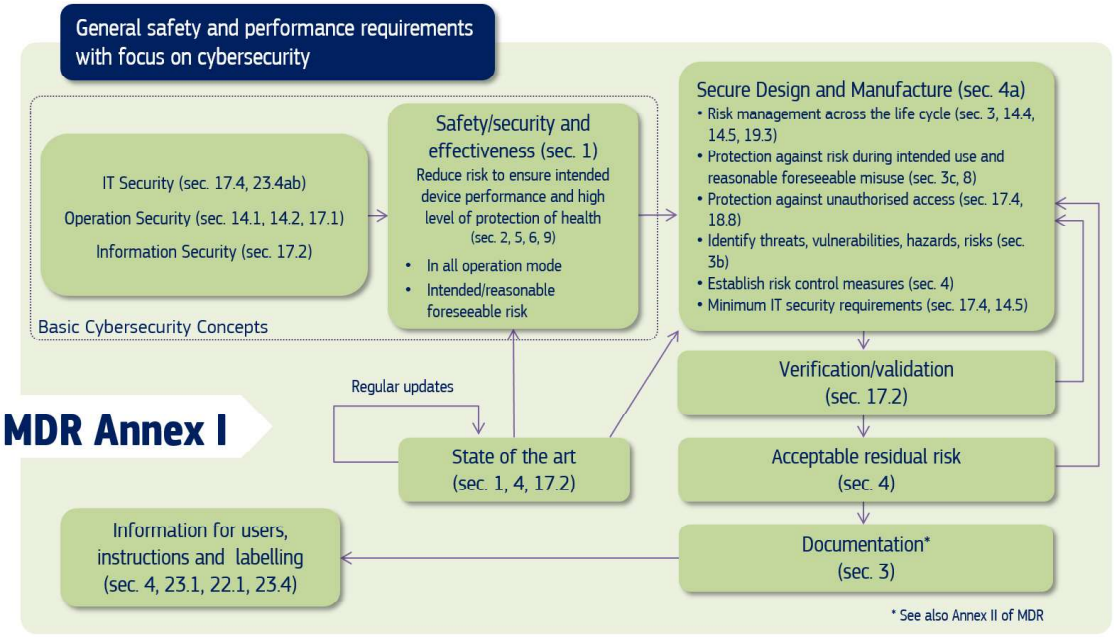

Figure 1: Cybersecurity requirements contained in MDR Annex I

The above requirements illustrated in Figure 1, are also applicable to those included in Annex I of Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices (IVDR). The correspondence between the sections in MDR Annex I and IVDR Annex I relevant for this guidance is provided in Table 1.

Table 1: Correspondence table between sections, relevant for this guidance, in MDR Annex I and IVDR Annex I

Main topic	Section number MDR Annex I	Section number IVDR Annex I
Device performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
Combination/connection of devices/systems	14.1	13.1
Interaction between software and the IT environment	14.2.d	13.2.d
Interoperability and compatibility with other devices or products	14.5	13.5
Repeatability, reliability and performance	17.1	16.1
Development and manufacture 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	17.2	16.2
Minimum IT requirements	17.4	16.4
Unauthorised access	18.8	-
Lay persons	22.1	-
Residual risks (information supplied by the manufacturer)	23.1 g	20.1 g
Warnings or precautions (information on the label)	23.2 m	20.2 m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4 g	-
Minimum IT requirements (information in the instructions for use)	23.4.ab	20.4.1.ah