European Commission

# The EU Medical Device Regulations and Cybersecurity

IHE Symposium
Rennes, 9 April 2019

**Salvatore Scalzo**
Health Technology and Cosmetics
DG Internal Market, Industry,
Entrepreneurship and SMEs
European Commission

# *Section 1:*
# *Regulation of medical software today*

# Legal background

Safety and performance requirements for software falling under the definition of a medical device (MDs) or an *in-vitro* diagnostic medical device (IVDs) are regulated by the respective directives:

- Directive 90/385/EEC (Active implantable MDs)
- Directive 93/42/EEC (MDs)
- Directive 98/79/EC (IVDs)

# Some important points to know

- A medical device is intended to have a medical purpose with an action other than pharmacological, immunological or metabolic.

- Software must fulfil the requirements of the medical devices legislation, also if no medical purpose but essential to enable the medical device to work or to assist its medical functionality (accessory).

- The Manual on Borderline and Classification clarifies that in the medical device regulatory context, apps are regulated as software.

# What happens if a software/app is a medical device?

- It must comply with the safety and performance requirements set in Annex I to the Directives

- Such compliance must be assessed through a specific conformity assessment procedure, which is proportional to the risk-class of devices:

- **For low-risk products (Class I), the manufacturer can provide a self-certification**
- **For all other products (Classes IIa, IIb and III), a control must be done by a Notified Body**

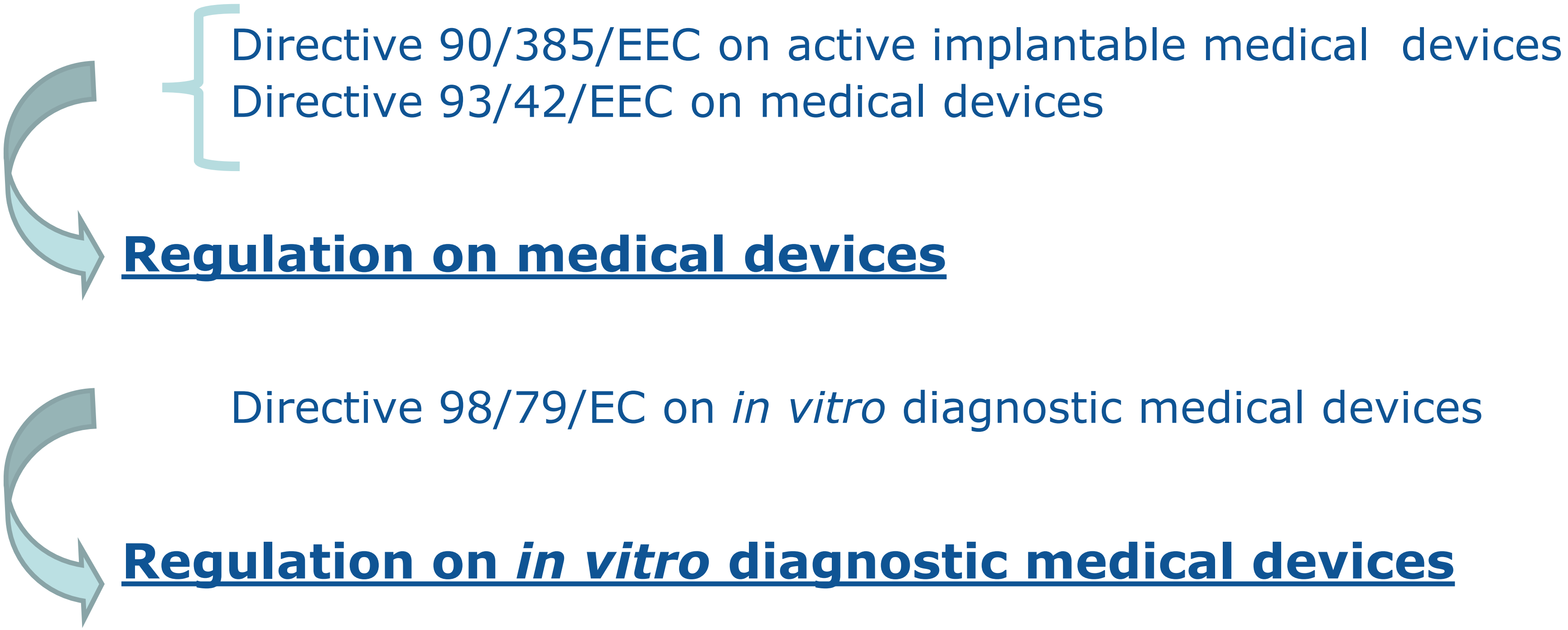
**-** Other requirements for manufacturers regard registration, post-market surveillance, incident reporting.

European Commission

# Section 2:
# The new Regulations on medical devices

# Revision of the EU Medical Devices Legislation

## Background



Directive 90/385/EEC on active implantable medical devices
Directive 93/42/EEC on medical devices

**Regulation on medical devices**

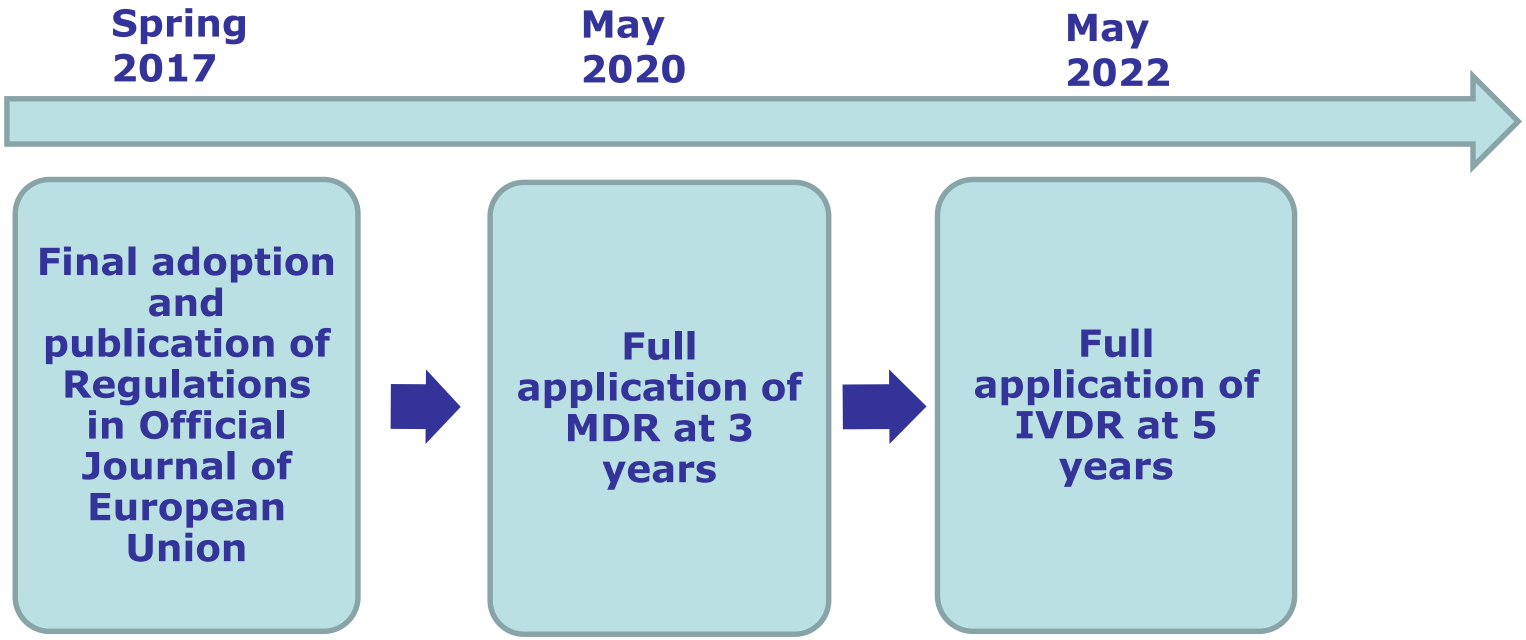
Directive 98/79/EC on *in vitro* diagnostic medical devices

**Regulation on *in vitro* diagnostic medical devices**

# Main features of the new texts

- ✓ **Stricter pre-market control** of high-risk devices with the involvement of a pool of experts at EU level.
- ✓ **Reinforced designation and oversight** processes of **notified bodies.**
- ✓ Reinforcement of the rules on **clinical evaluation** (and performance evaluation) and **clinical investigation** (and performance studies).
- ✓ **New classification system for IVDs** based on international guidance (80% of IVDs to be assessed by a Notified Body).
- ✓ **Establishment of a comprehensive EU database on medical devices (EUDAMED)** with large part of information to be made publicly available.
- ✓ Stricter requirements related to the **use of hazardous substances** for certain devices.
- ✓ Clarification of the role and responsibilities of **economic operators**.
- ✓ Inclusion of **certain aesthetic devices** within the **scope**.
- ✓ EU minimum requirements related to **reprocessing of single-use devices**.
- ✓ Introduction of a **UDI system**.

# Transitional period



Spring 2017

May 2020

May 2022

Final adoption and publication of Regulations in Official Journal of European Union

Full application of MDR at 3 years

Full application of IVDR at 5 years

# *Section 3: Impact of MDR on medical software and new requirements on cybersecurity*

# Main features of the new MDRs

1. Definition of "medical device"
2. New classification rules (obligation for clinical investigation)
3. UDI requirements for software
4. Dedicated general safety and performance requirements (including cybersecurity)

# Safety and performance requirements (Annex I) related to cybersecurity

***17.1** Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to **ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.***

***17.2** For devices that incorporate software or for software that are devices in themselves, **the software shall 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.*

***17.4 Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended***

***23.4 The instructions for use shall contain all of the following particular:***

***[…]***

*(ab) for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, **minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.***

# Work of the EU Expert Group on medical software in the cybersecurity field 1/2

- ✓ Task-force on cybersecurity established in spring 2018 (first meeting 31 May) – it is coordinated by DG GROW in cooperation with ENISA and JRC and includes experts from Member States, industry and healthcare institutions
- ✓ Mission:
  - ✓ to provide a platform for discussion and possibly develop a guidance for manufacturers
- ✓ Expected duration: 18 month
- ✓ Steps of the project:
  - ✓ Review of existing regulation (at both EU and MS level) between May and October 2018
  - ✓ Discussion on review outcomes on 25 October 2018
  - ✓ Draft of guidance starting from November 2018
  - ✓ Next meeting of the TF foreseen on 6 May 2019

# Work of the EU Expert Group on medical software in the cybersecurity field 2/2

- ✓ Focus of guidance:
  - ✓ Description of general principles on cybersec (including shared responsibility, importance of intended use and intended environment) and legal background
  - ✓ Description of risk management process in relation to cybersecurity
  - ✓ Considerations of cybersecurity principles in design/development
  - ✓ Minimum requirements on IT concerning hardware, IT networks characteristics and IT security measures and communication issues with operators/users
  - ✓ Consideration on operators (other than Manufacturers)

# Section 4:
# Recent developments at international level

# New IMDRF Work Item on cybersecurity

- ✓ The **International Medical Device Regulators Forum (IMDRF)** is a voluntary group of medical device regulators from around the world who aim to accelerate international medical device regulatory harmonization and convergence
- ✓ **New Work Item Proposal on cybersecurity** adopted at the IMDRF Management Committee meeting in September 2018
- ✓ **Purpose**: To facilitate international regulatory convergence on medical device cybersecurity with open discussion and sharing best practices that are understandable and feasible for all stakeholders supporting innovation and timely access to safe and effective medical devices globally
- ✓ **Main issues to be addressed**: Recognition of cybersecurity as a shared-responsibility; Promote broad information-sharing policies; definition of relevant regulatory terms
- ✓ Duration: to be completed by March 2020

**Thank you
for your attention**