TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Cyber4Health Observatory

prof. Gaetano Marrocco, chair Medical Engineering Degree

Ing. Francesco Lestini, **Ing. Francesca Nanni**, PhD Students

Università di Roma Tor Vergata

Contact: Gaetano.marrocco@uniroma2.it

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

MEDICAL DEVICE

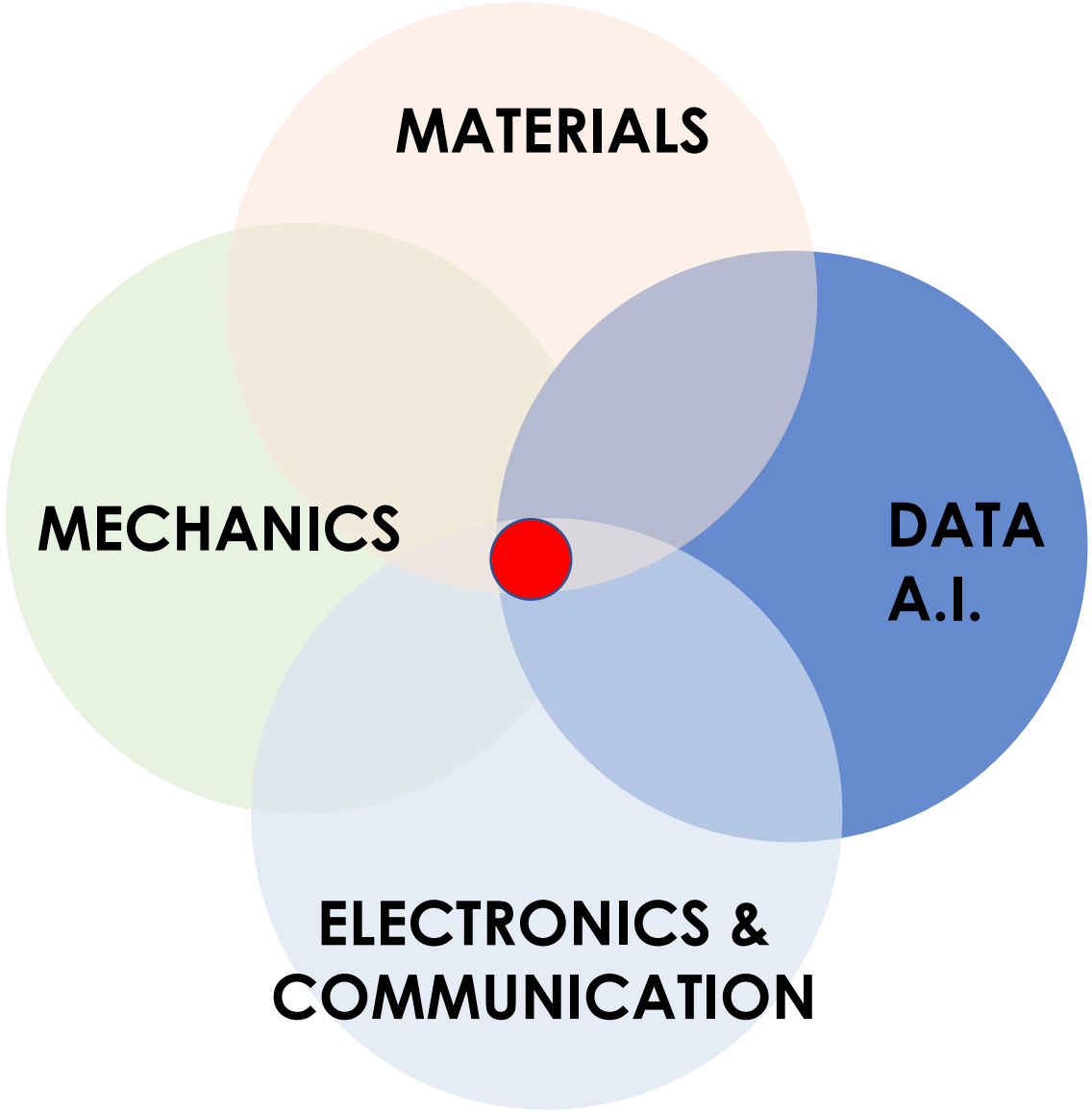
A medical device

is a product used for diagnosis, prevention, monitoring, treatment or alleviation of disease or injury in humans.

Can be :

- a physical object
- a software or
- a combination of both.

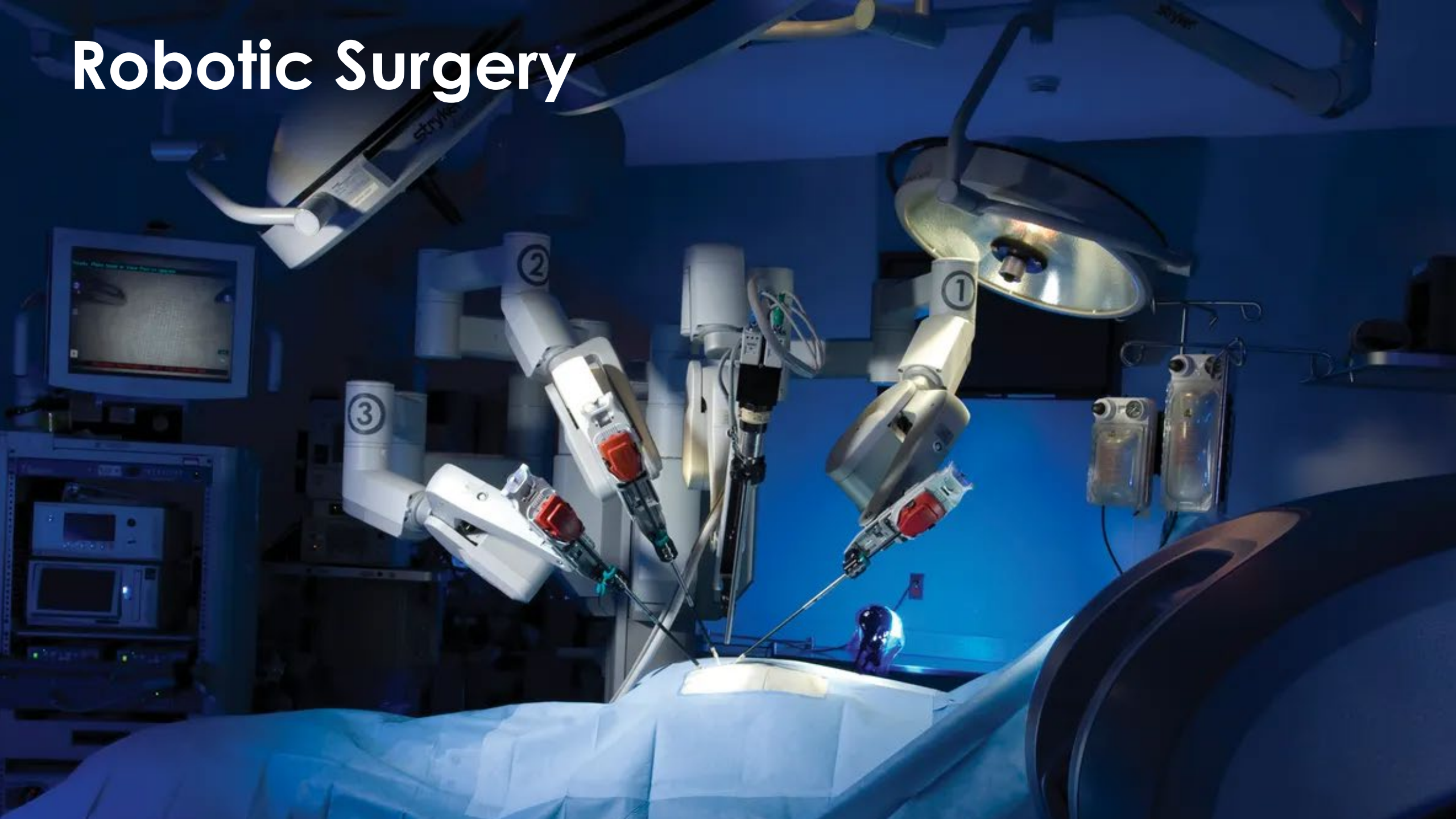
MD originally played a physical action, but the are now becoming generator and repository of very sensitive data.



(https://ec.europa.eu/growth/sectors/medical-devices_it)

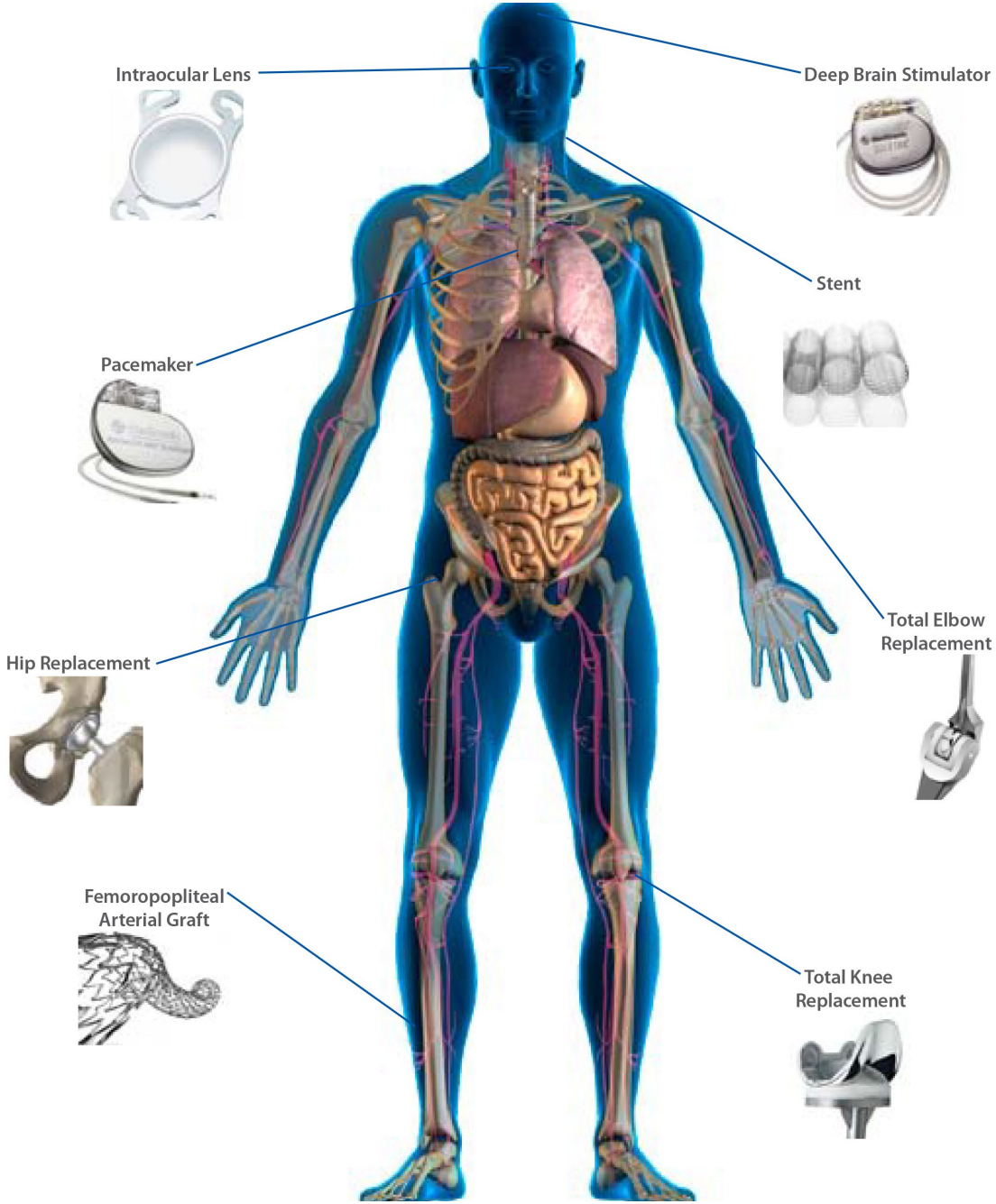
Advanced Diagnostics

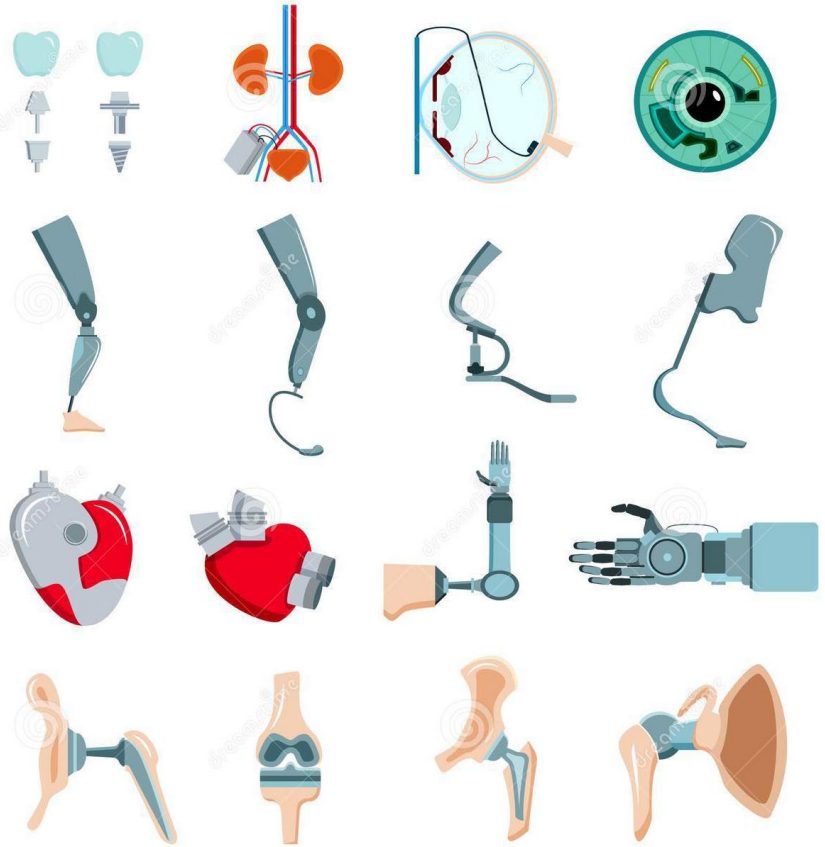
Robotic Surgery



TOR VERGA
UNIVERSITÀ DEGLI STUDI DI

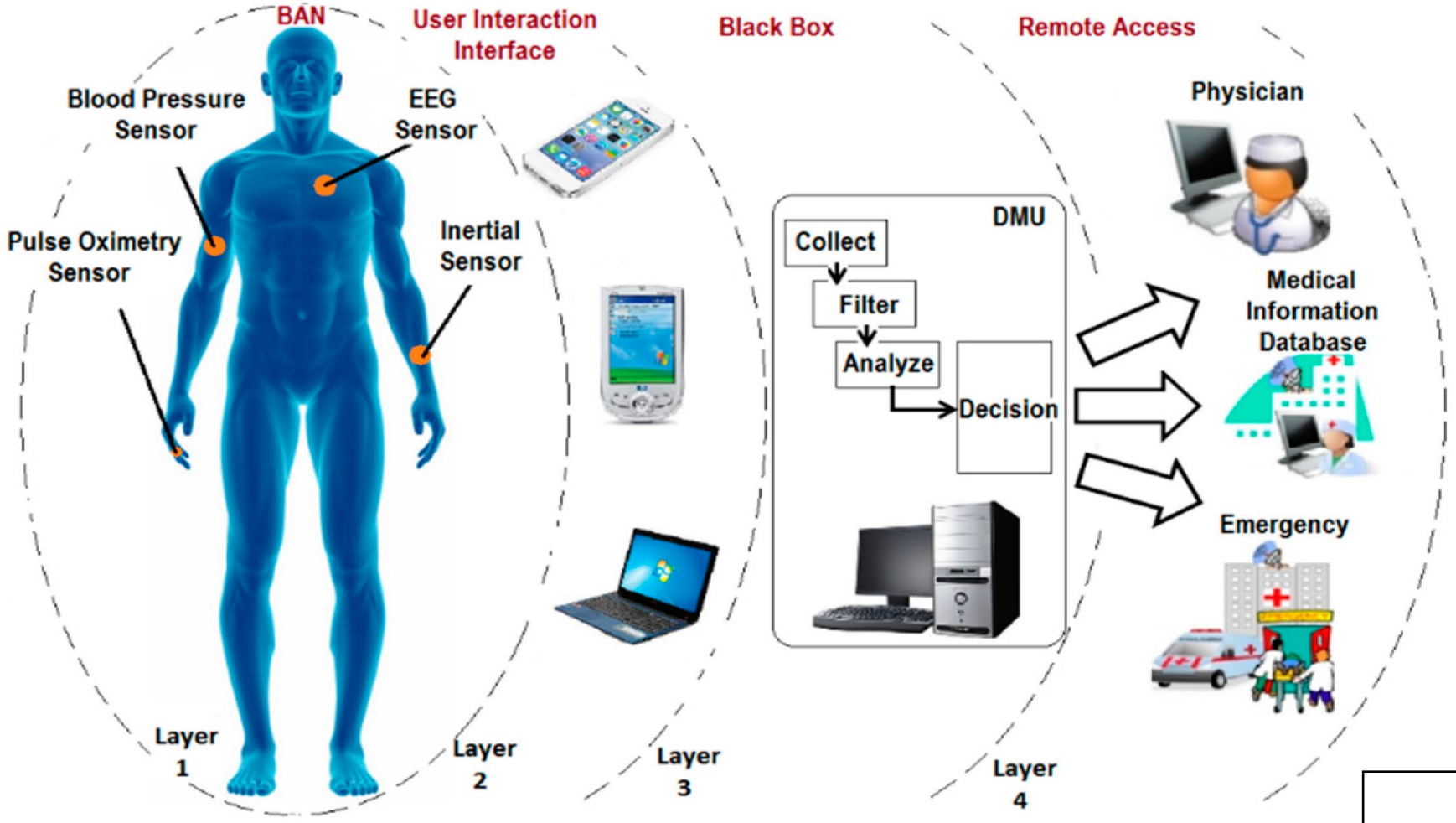
Medical Implants (Endo-prosthesis)





TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Wireless/Wired Connectivity



- Configuration & SW upgrade
- Data retrieval
- Actuation

Potential Non-authorized Interactions

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Cyber and Physical security

Cyber Security

*Protection from attacks to devices/devices made by means of **Software Systems/procedures***

Physical Security

*Protection from attacks to devices made by means of **Hardware Systems/procedure***

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Scenario

2010

At a Black Hat conference Barnaby Jack gave a presentation on **"jackpotting"** or causing automated teller machines to dispense cash without withdrawing it from a bank account using a bank card

2011

At the McAfee FOCUS 11 conference in October **2011** in Las Vegas, Jack first demonstrated the **wireless hacking of insulin pumps**

2012

Jack asserted that he could assassinate a victim by **hacking their pacemaker**

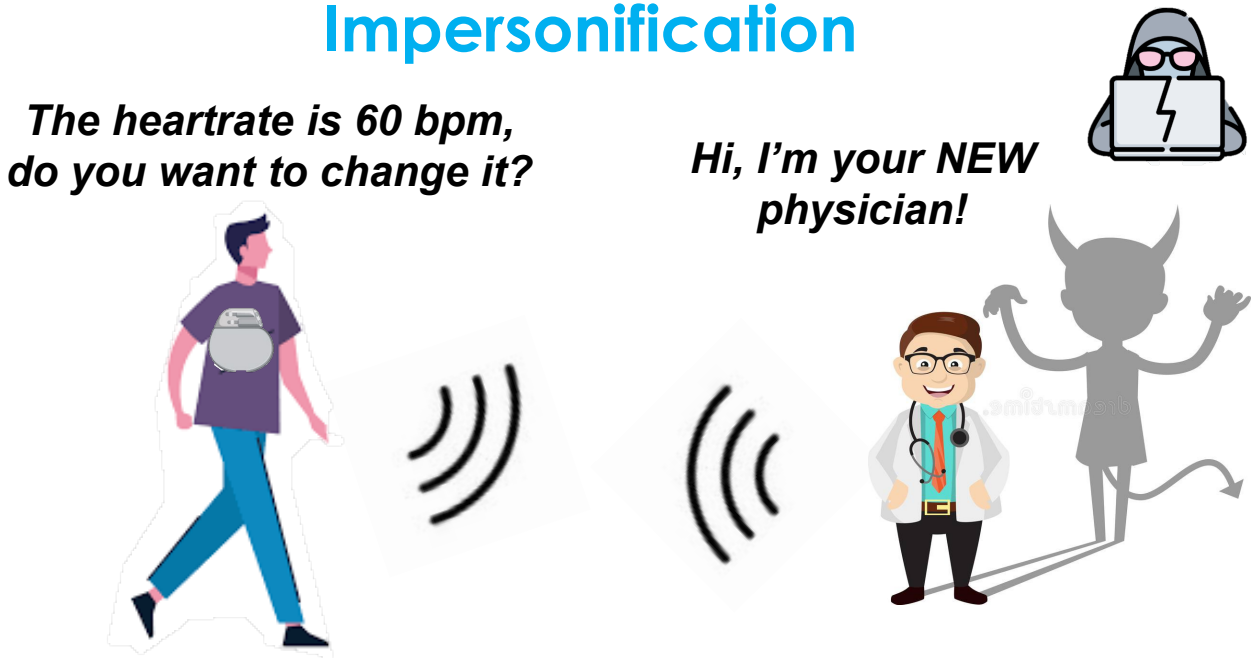
2018

Billy Rios and Jonathan Butts (Rapid7) demonstrated they've found vulnerabilities that **compromised the pacemaker's programmer**

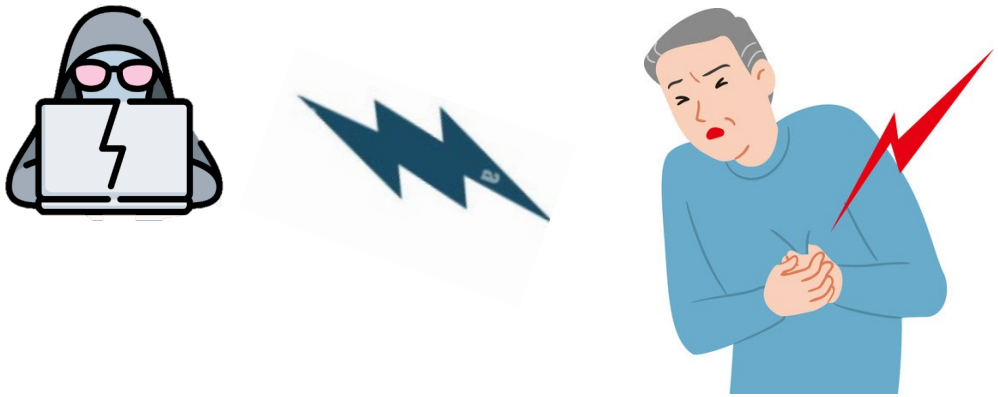
Electromagnetic Attacks

Eavesdropping

Impersonification

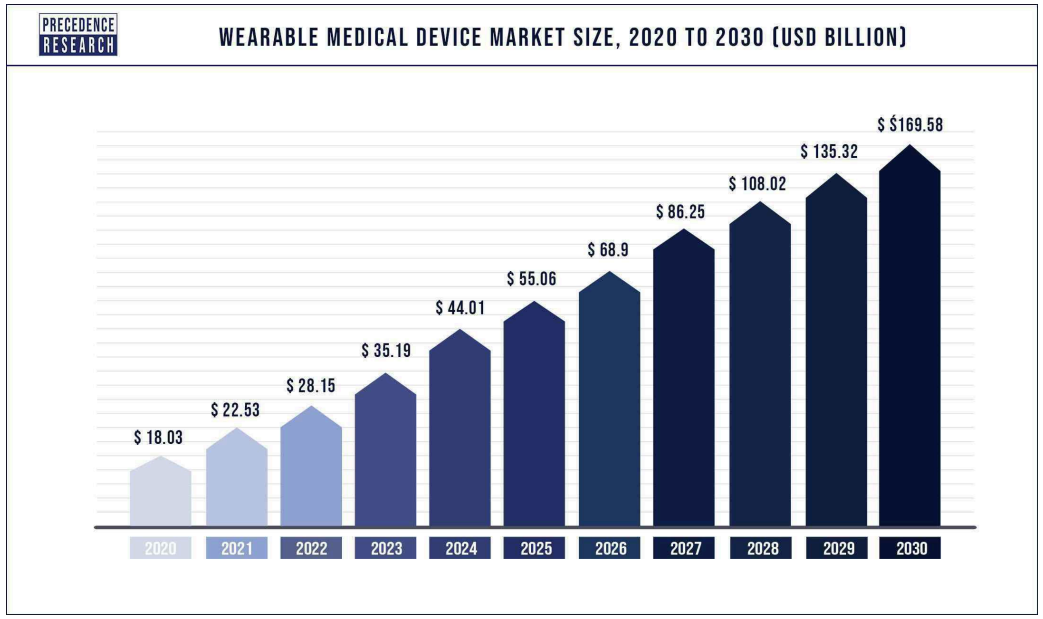


Fault induction attack

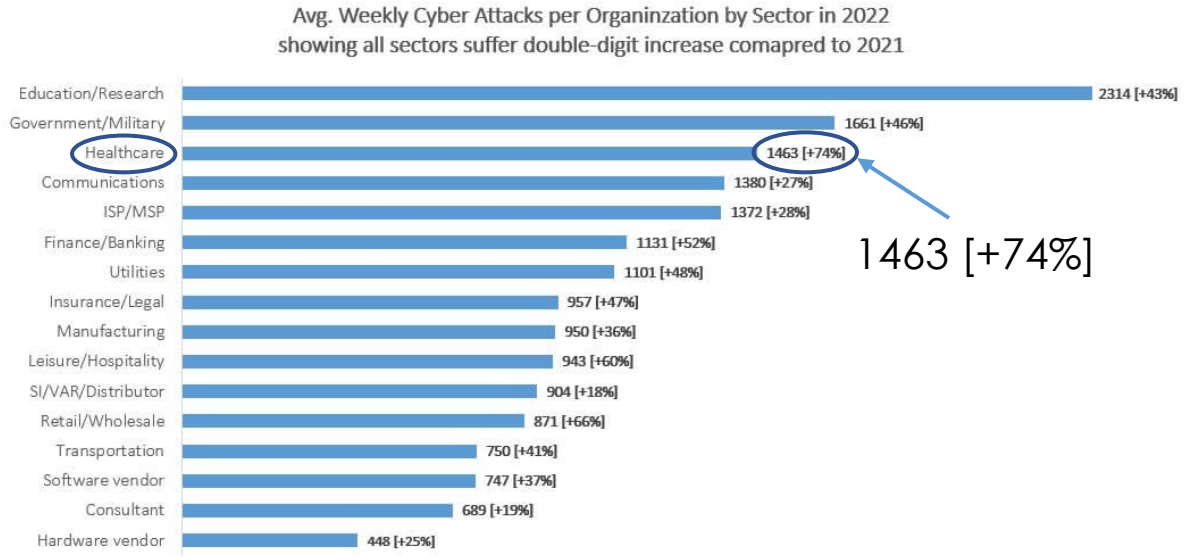


Resource Depletion

The urgence of an Open Observatory on Cyber-physical Vulnerability of M.D.



The global wearable medical devices market size was estimated at **USD 28.15 billion in 2022** and is expected to hit **over USD 169.58 billion by 2030.**



The healthcare industry is among the **preferred target of cyber attackers** because of the **high commercial value of EHRs** (electronic health records).

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Mission

Information Gathering and Sharing:
Implement a platform capable of enabling structured information sharing specifically for cyber threats in the medical sector.

Services Providing: Provide a reference for those involved in technology development, certification, maintenance, and marketing of medical devices (MDs) regarding current cyber threats.

Awareness Raising: Make this information usable and easily understandable by patients and caregivers.

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Sources

GOVERNMENT ORGANIZATION

Involved in disseminating such information, especially American ones (H-ISAC, FDA, CISA...).

SCIENTIFIC PAPERS

Papers and books that technically describe the vulnerabilities (especially physical) of a medical device and/or assess its security through *penetration testing*.

NEWSPAPER ARTICLES

News about cyber incidents to medical devices or healthcare infrastructures.

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Classification

Body-district

- **Stomach**
- Fingers
- Head
- **Hearth**
- Wrist
- Feet
- Arms
- External
- Variable

Product

- Insulin pump
- Oximeter
- **Pacemaker**
- Smartwatch
- Hospital network
- Software/Application
- **MRI, CT, Ultrasound…**

Attack

- Eavesdropping
- **MITM**
- DDOS
- Brute Force
- Unauthorized Access
- **Sniffing**
- Spoofing…

Device

- **Implantable**
- Wearable
- Smartwatch
- **On-site medical equipment**

Year

Vulnerability

- **Cyber**
- **Physical**

Severity (CVSS)

- **From 1 to 10**

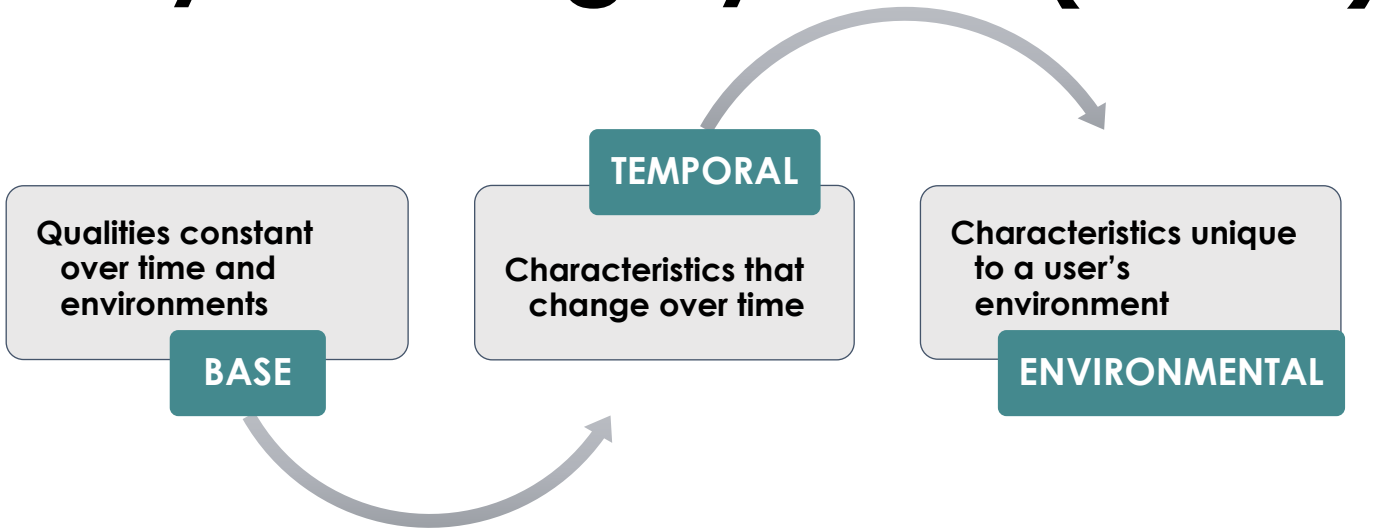
Risk Class

- **Class I**
- Class IIa
- Class IIb
- **Class III**

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a method used to supply a **qualitative measure of severity**. CVSS **is not a measure of risk** and consists of three metric groups.



NIST
National Institute of Standards and Technology

CVSS is owned by **FIRST.Org**, but **NIST** provides a **National Vulnerability Database (NVD)** with qualitative severity ratings of score ranges. The NVD does not currently provide temporal or environmental scores.

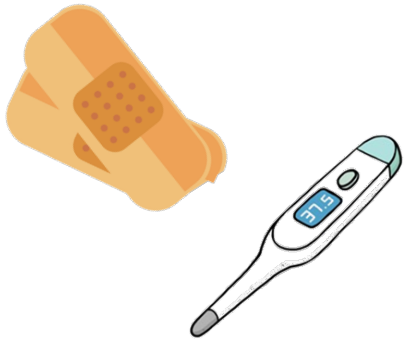
SEVERITY	None	Low	Medium	High	Critical
CVSSv3.0 SCORE	0.0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 – 10.0

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

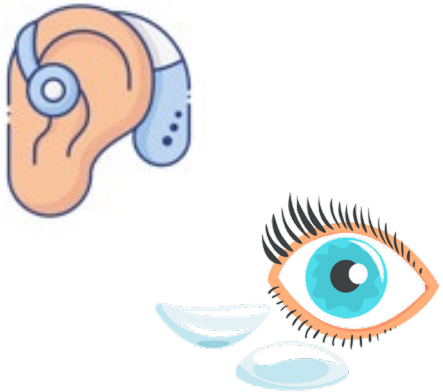
Risk class

According to the **EU Regulation 2017/745** of the European Parliament and of the Council of 5 April 2017, effective on 26 May 2021, medical devices are classified in four classes based on the level of **safety risk** they pose to patients and users.

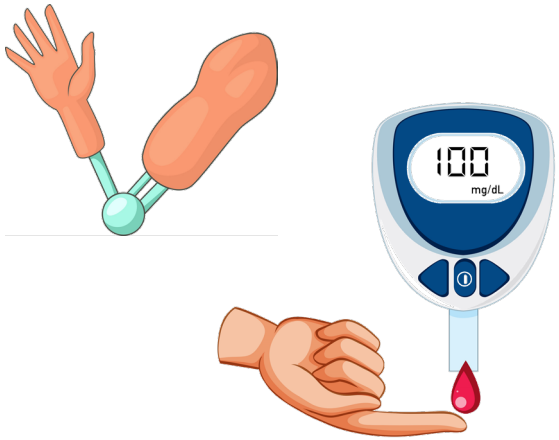
CLASS I
Low risk



CLASS IIa
Medium risk



CLASS IIb
High risk



CLASS III
Highest risk

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Safety and Security

FIRST™ Improving Security Together

CVSS

RISK CLASS

European Commission
Medical Devices Regulation
EU MDR

When a medical device suffers from a security breach,
a security issue becomes a safety issue.

TOR VERGATA UNIVERSITY OF ROME

CYBER4HEALTH

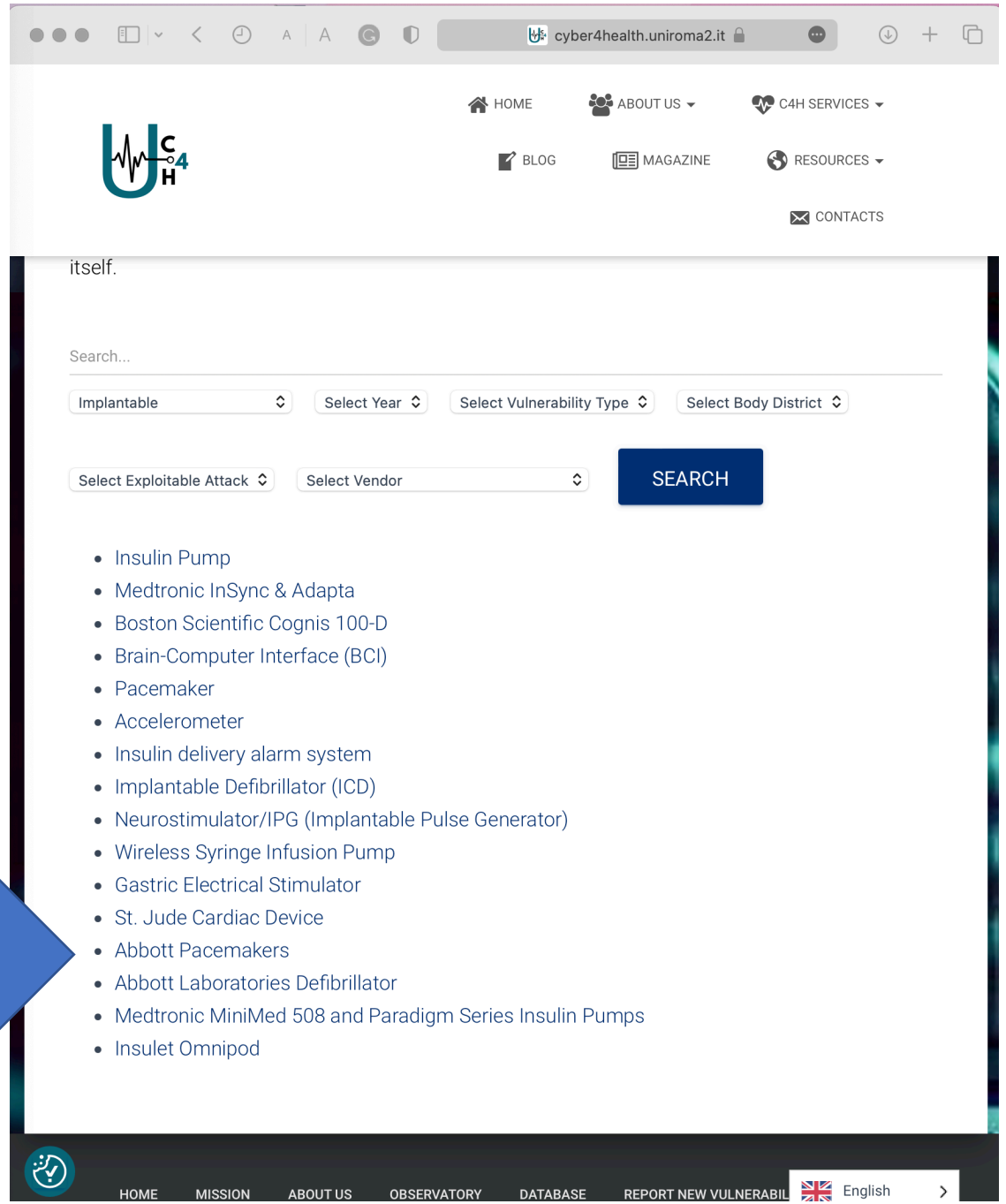
Information Center to encourage medical devices' Security by Design

READ MORE

LEARNING QUERY STATISTICS SUBMIT

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

QUERY



Vulnerability Description

Device Name
Abbott Pacemakers

Vendor
Abbot

Product Name
Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI.

Product Type
pacemaker

Body-District Application
Heart

Taxonomy of the attack
Unauthorized Access, Information Disclosure, Tampering, Resource Depletion

CVSS
7

Vulnerabilities
Improper authentication mechanism, missing ecnryption, improper restriction of power consumption

Type of the attack
Cyber

Type of Device
Implantable

Year
2017

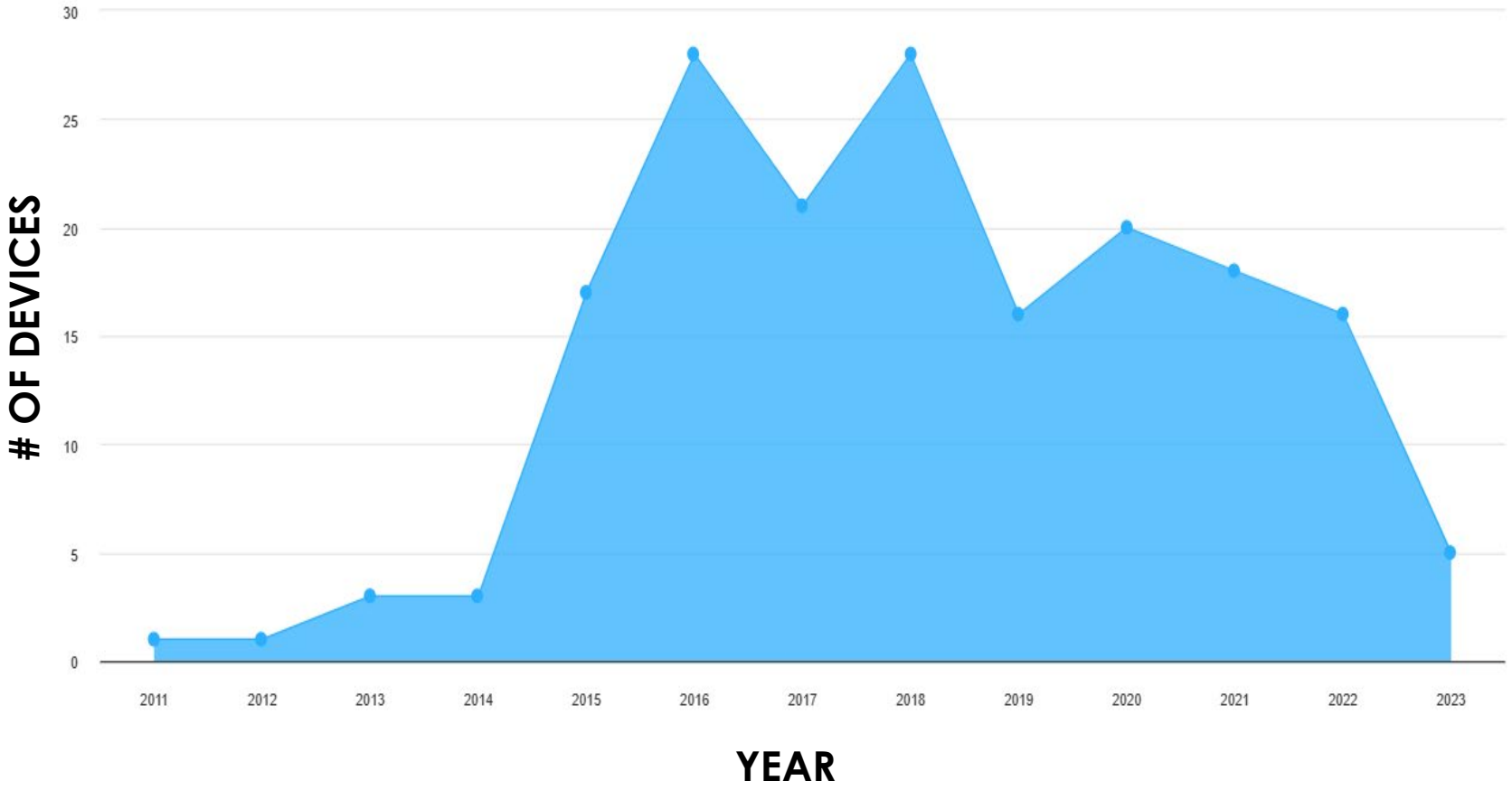
Description
Successful exploitation of these vulnerabilities may allow a nearby attacker to gain unauthorized access to a pacemaker and issue commands, change settings, or otherwise interfere with the intended function of the pacemaker. The pacemaker's authentication algorithm, which involves an authentication key and time stamp, can be compromised or bypassed, which may allow a nearby attacker to issue unauthorized commands to the pacemaker via RF communications. The pacemakers do not restrict or limit the number of correctly formatted "RF wake-up" commands that can be received, which may allow a nearby attacker to repeatedly send commands to reduce pacemaker battery life. The Accent and Anthem pacemakers transmit unencrypted patient information via RF communications to programmers and home monitoring units. The Assurity and Allure pacemakers do not contain this vulnerability. Additionally, the Accent and Anthem pacemakers store the optional patient information without encryption; however, the Assurity and Allure pacemakers encrypt stored patient information. These vulnerabilities could be exploited via an adjacent network. Exploitability is dependent on an attacker being sufficiently close to the target pacemaker as to allow RF communications.

Countermeasures
Abbott has developed a firmware update to help mitigate the identified vulnerabilities. The pacemaker firmware update will implement "RF wake-up" protections and limit the commands that can be issued to pacemakers via RF communications. Additionally the updated pacemaker firmware will prevent unencrypted transmission of patient information (Accent and Anthem only). The firmware update can be applied to an implanted pacemaker via the Merlin PCS Programmer by a healthcare provider. It is recommended that healthcare providers discuss this update with their patients and carefully consider the potential risk of a cybersecurity attack along with the risk of performing a firmware update. Implementation of the firmware update is to be determined based on the physician's professional judgment and patient management considerations. Pacemakers manufactured beginning August 28, 2017, will have this update preloaded on devices. Abbott states that firmware updates should be approached with caution. Like any software update, firmware updates can cause devices to malfunction. Potential risks include loss of device settings, the device going into back-up mode, reloading of the previous firmware due to a failed upgrade, loss of diagnostic data, and a complete loss of device functionality. The Abbott Cybersecurity Medical Advisory Board has reviewed this firmware update and the associated risk of performing the update in the context of potential cybersecurity risk.

References
https://www.cisa.gov/uscert/ics/advisories/ICSMA-17-241-01

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

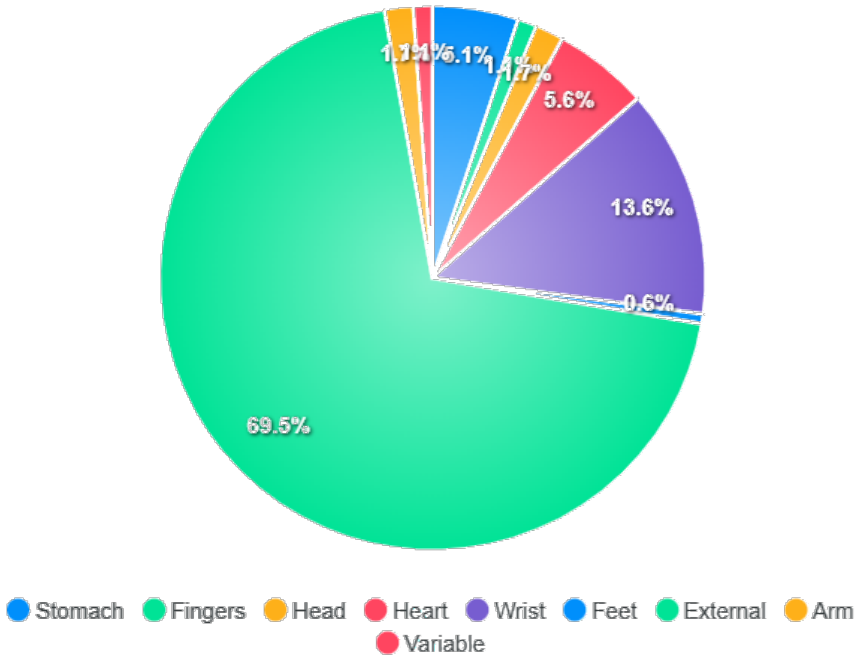
Attack/Vulnerability per Year



A peak between **2016** and **2018.**

Drop during the **COVID-19 pandemic**, probably due to increase in resources enhancing network security (telemedicine, remote lessons...)

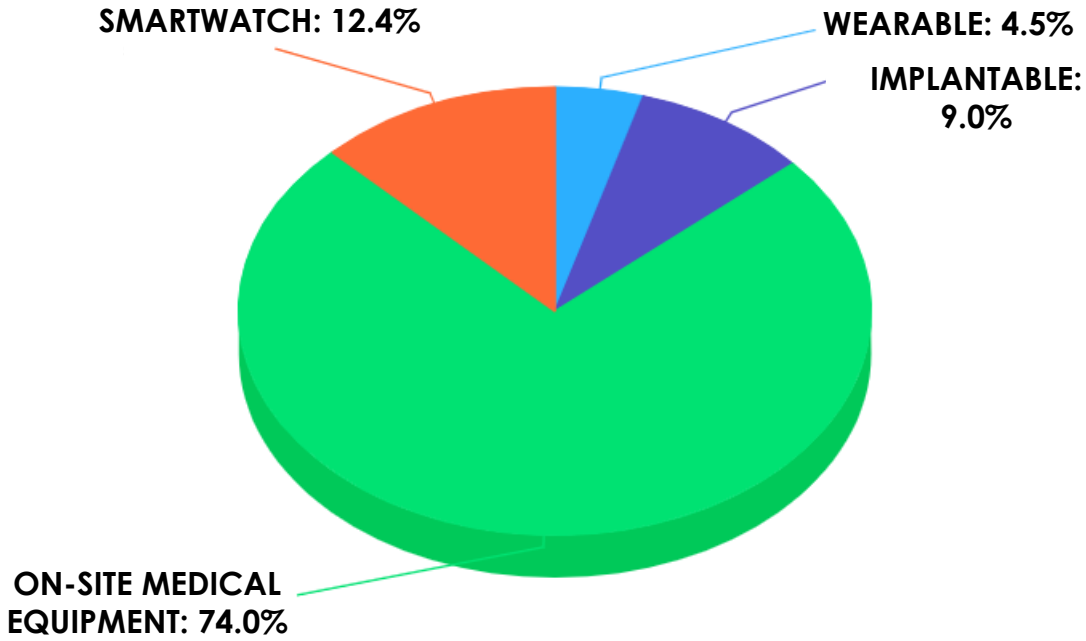
Vulnerability vs Body-District and device type



Most of vulnerabilities are related to external devices (on-site medical equipment).

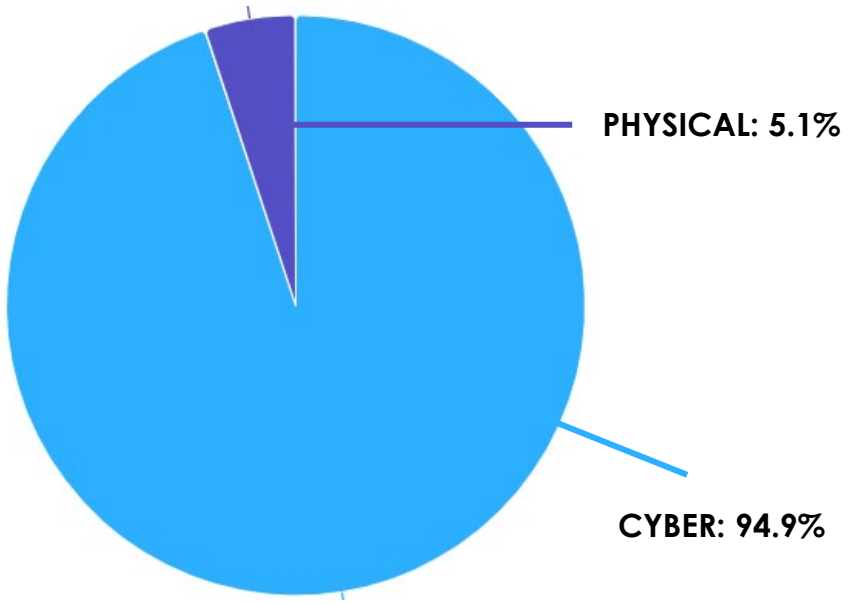
an attacker is always interested in **monetary profit**. Therefore, attacking an on-site device is much more valuable than attacking the individual patient since it would allow much more sensitive data to be obtained.

The most vulnerable **types** of devices are **on-site medical equipment** followed by smartwatches because they are easier to attack than wearable and implanted devices and contain a lot of **sensitive data**.



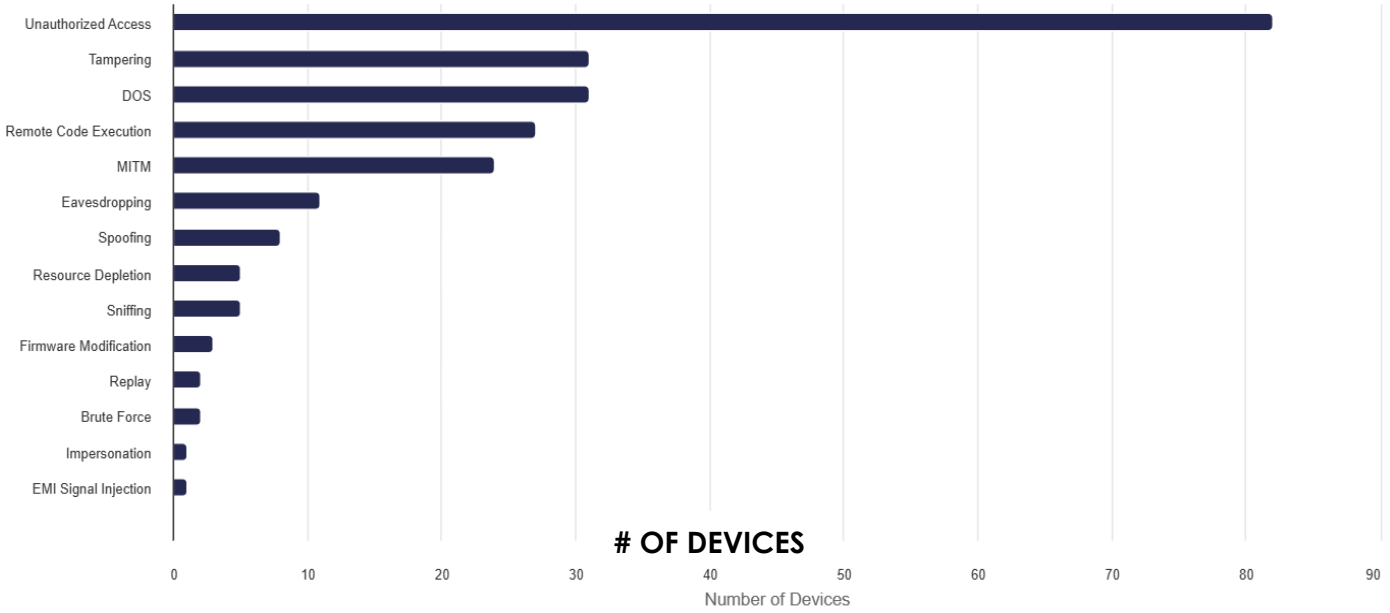
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Type of attacks



Vulnerabilities are almost all **cyber**. This is because they can be **remotely exploited**,

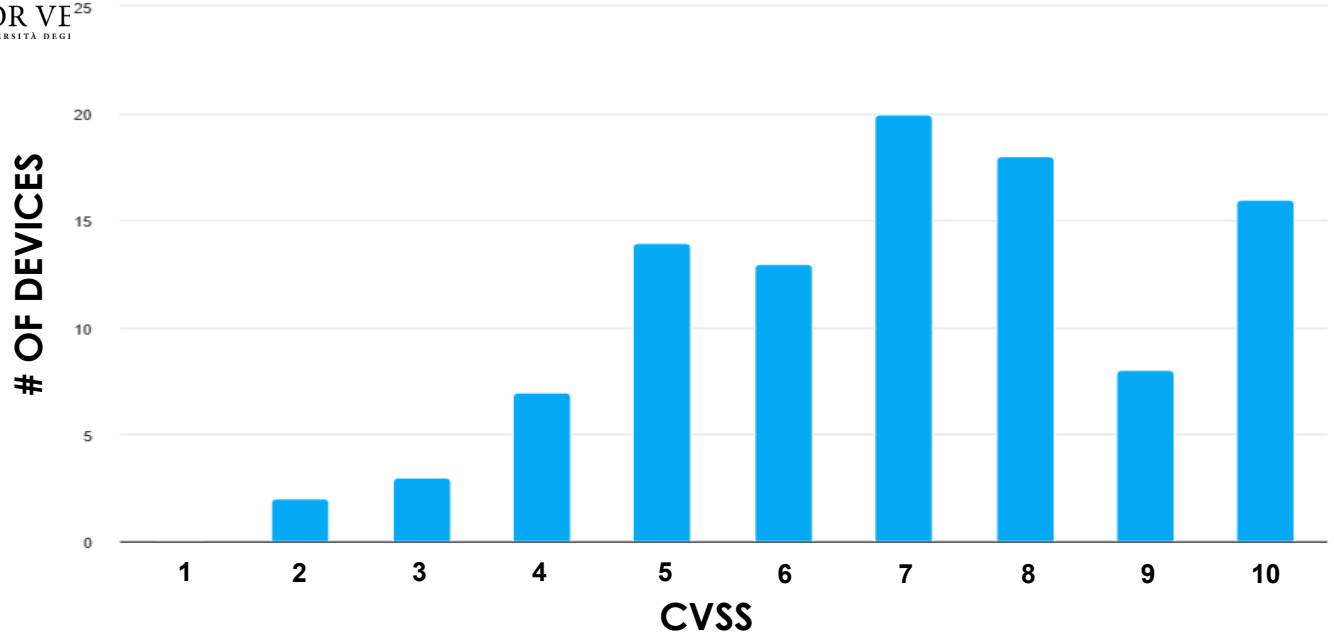
Physical vulnerabilities are generally difficult to exploit, and at the same time **almost impossible to detect.**



The most common type of attack is **unauthorized access**, which can be physical access in certain areas of hospitals or to PCs containing sensitive data, or by hacker attacks (**phishing**).

Among the first 4 there is the **remote code execution** which is the most dangerous because it gives you total access to the device.

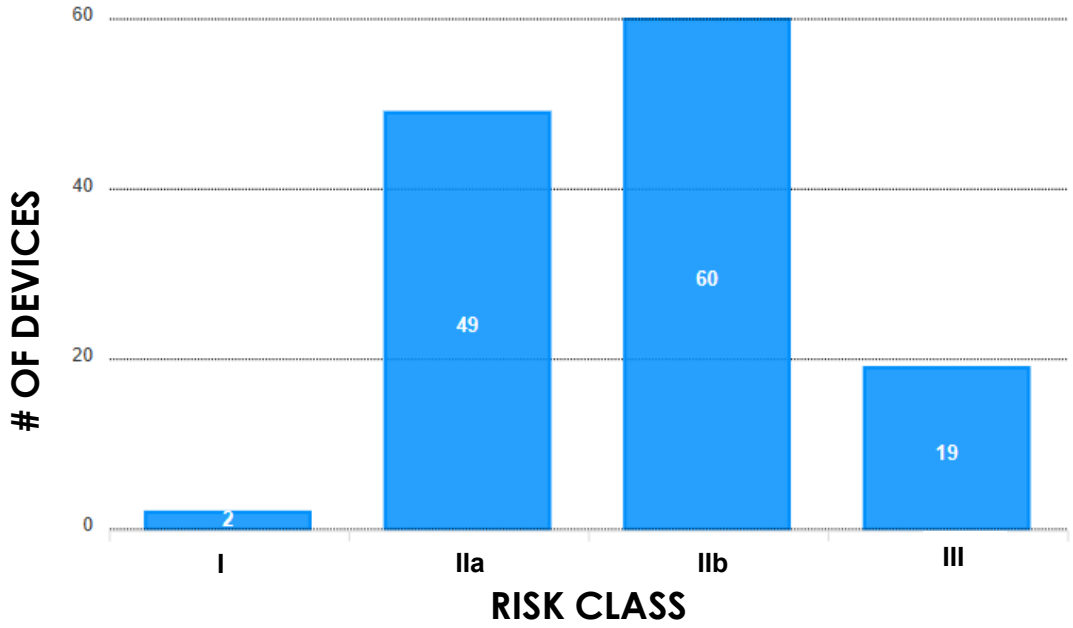
Security and Safety



Most vulnerabilities have a **CVSS between 7 and 10**. This means that they can be exploited by a **low-skilled** attacker with low-cost instrumentation.

Devices are almost all **class IIa and IIb**, but there are also many **class III.**

If there is a vulnerability, it is a serious one and it is also very dangerous to the patient's health.



TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Take-home message

Medical device of the near future:

- Bio-integrated
- Pervasive
- Physical /Digital
- Wireless Interconnected

Needs:

- **Understand** source of Vulnerabilties
- **Correlate** their impacts with the Safety and the Privacy of the User/Patient

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Thanks for attending !

Gaetano.marrocco@uniroma2.it
www.pervasive.ing.uniroma2.it

CYBER4 HEALTH

Pervasive Electromagnetics Lab

https://cyber4Health.uniroma2.it