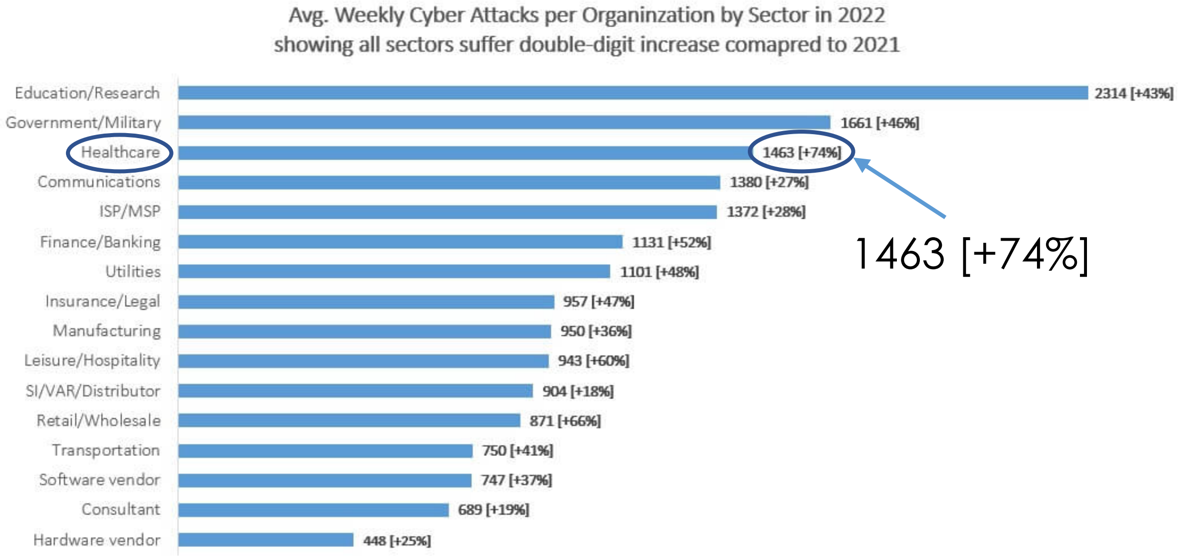
Cyber4Health Observatory: Live Demo and Statistics

Ing. Francesco Lestini

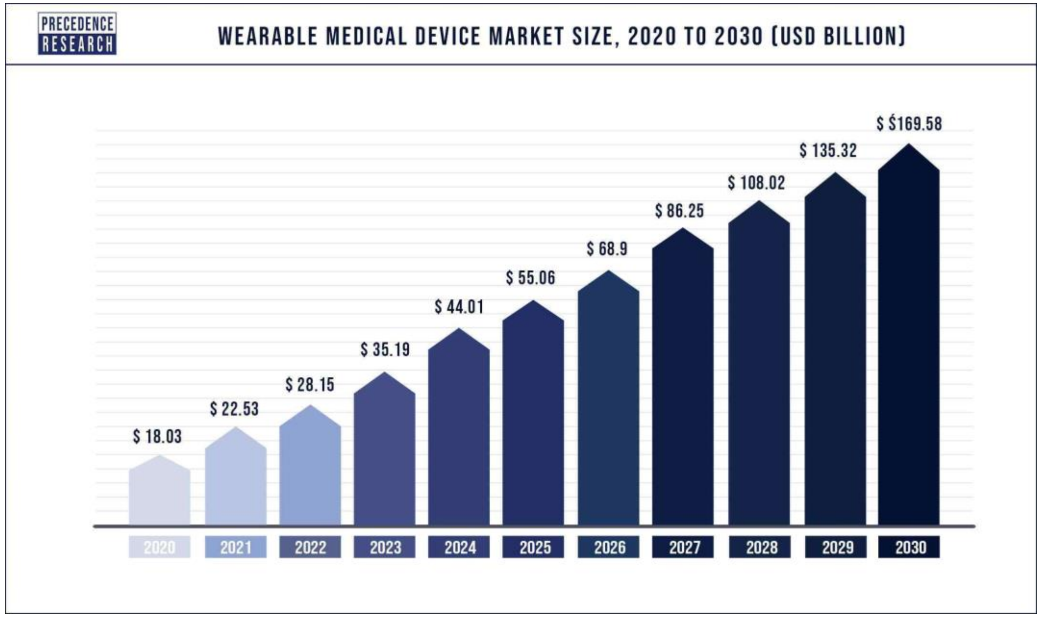
Contact: *francesco.lestini@uniroma2.it*

Motivations

The healthcare industry is among the **preferred target of cyber attackers** because of the **high commercial value of EHRs**.



1463 [+74%]



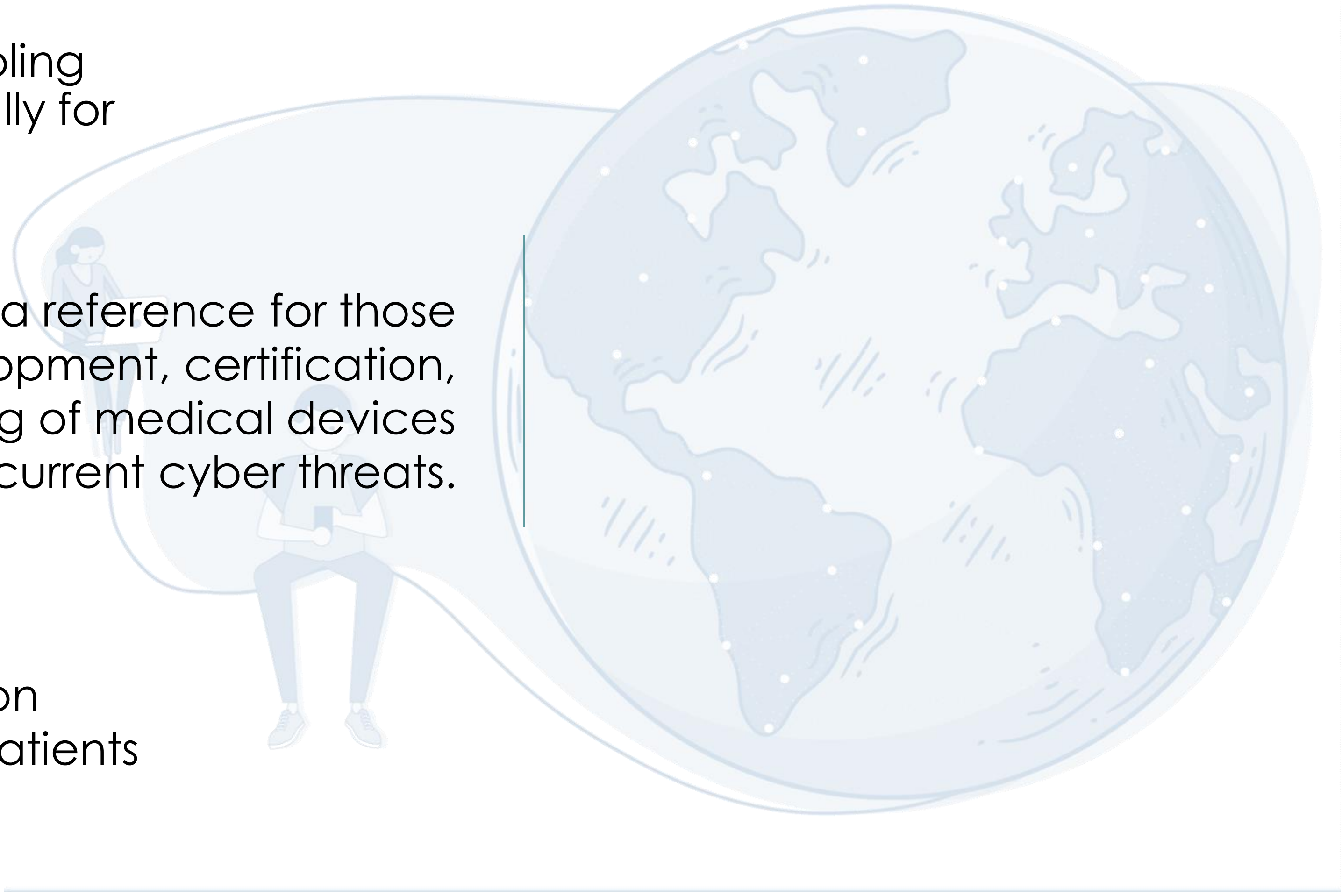
The global wearable medical devices market size was estimated at **USD 28.15 billion in 2022** and is expected to hit **over USD 169.58 billion by 2030.**

Goals

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.



Development

PHASE I RESEARCH

Research all available information regarding cyber incidents and vulnerabilities of a medical device.

PHASE II COLLECT

Collect and organize the found data in a database.

PHASE III CLASSIFY

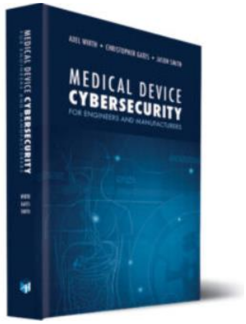
Classify data according to fields that are meaningful and able to offer clear and simple interpretations.

Sources

GOVERNMENT ORGANIZATION

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

SCIENTIFIC ARTICLES


AXEL WIRTH • CHRISTOPHER GATES • JASON SMITH
MEDICAL DEVICE CYBERSECURITY
FOR ENGINEERS AND MANUFACTURERS

Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors

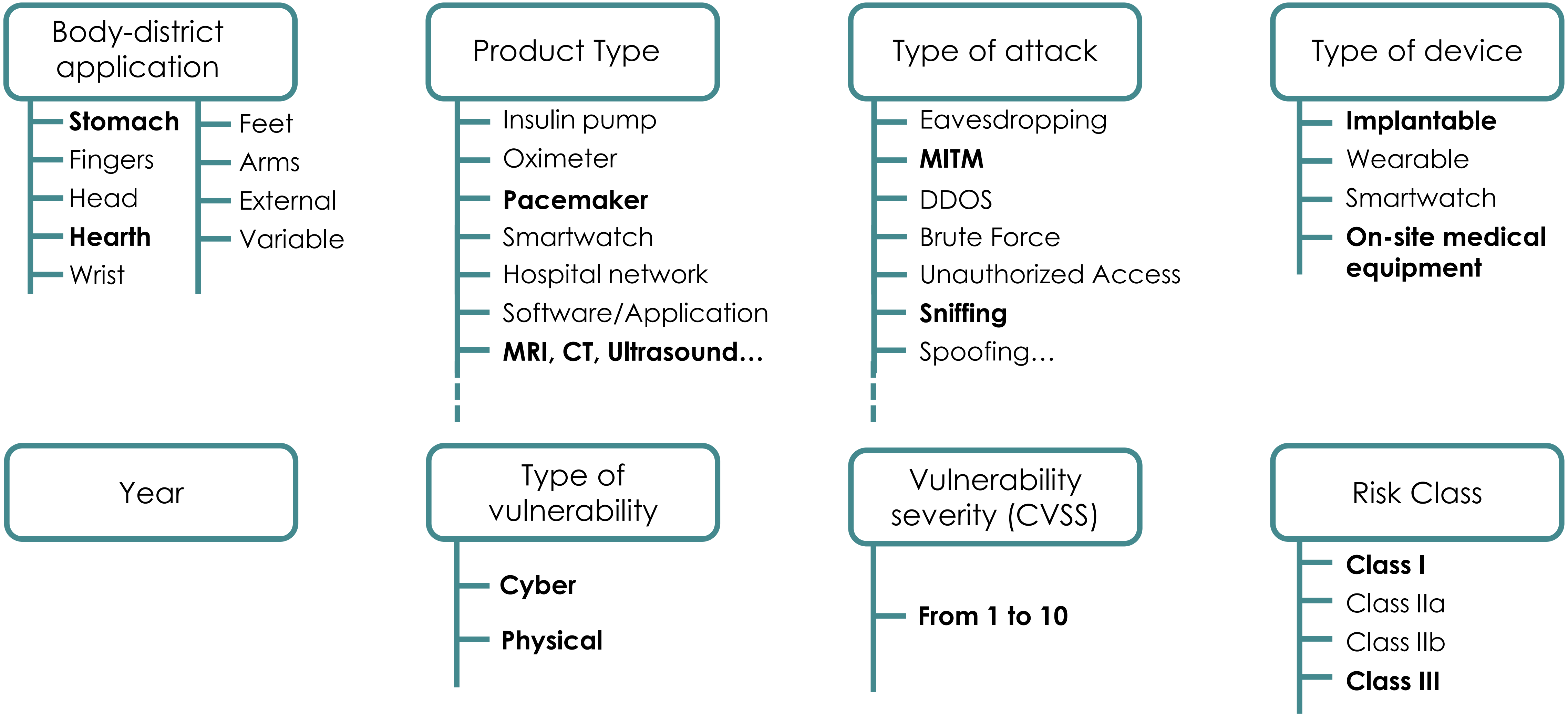
Papers and books that technically describe the vulnerabilities (especially physical) of a medical device and/or assess its security through *penetration testing*.

NEWSPAPER ARTICLES

News about cyber incidents to medical devices or healthcare infrastructures.

The untold story of a cyber attack, a hospital, and a dying woman

Data Classification



Body-district application

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

Product Type

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

Type of attack

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

Type of device

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

Year

Type of vulnerability

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

Vulnerability severity (CVSS)

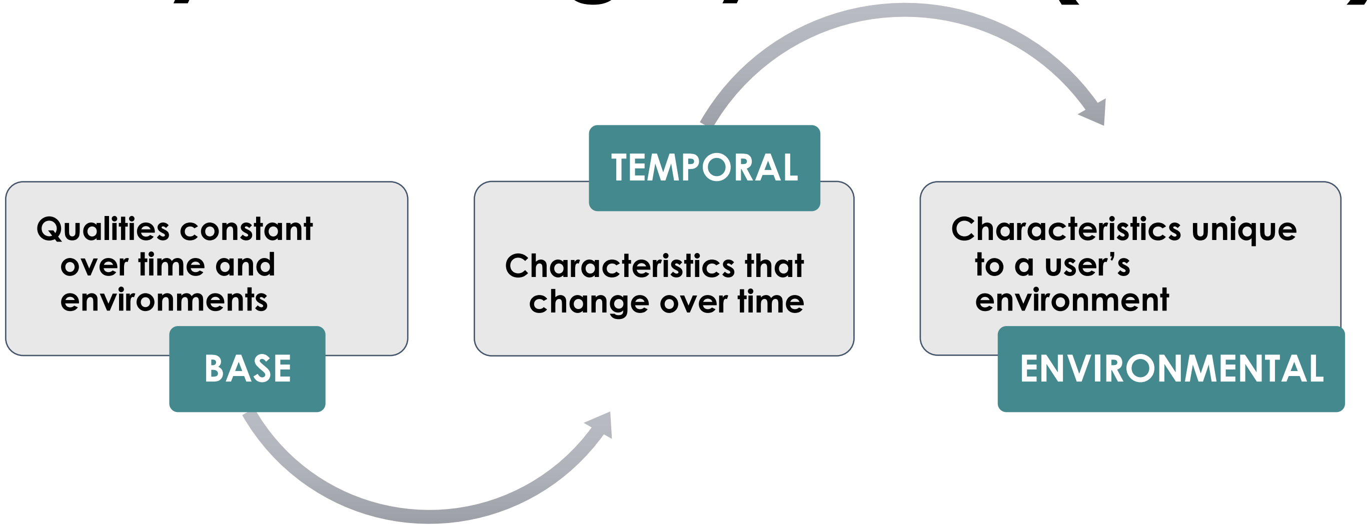
- **From 1 to 10**

Risk Class

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

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.



BASE – Qualities constant over time and environments

TEMPORAL – Characteristics that change over time

ENVIRONMENTAL – Characteristics unique to a user's environment

NIST
National Institute of Standards and Technology

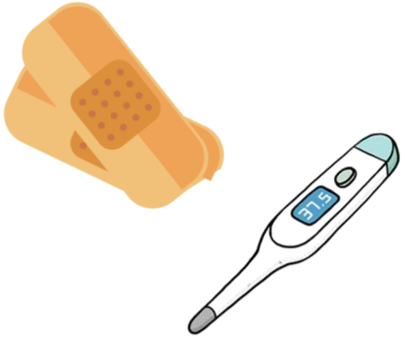
CVSS is owned by **FIRST.Org**, but **NIST** provides a **National Vulnerability Database (NVD)** with qualitative severity ratings of score ranges. The NVD does not currently provide temporal or environmental scores.

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

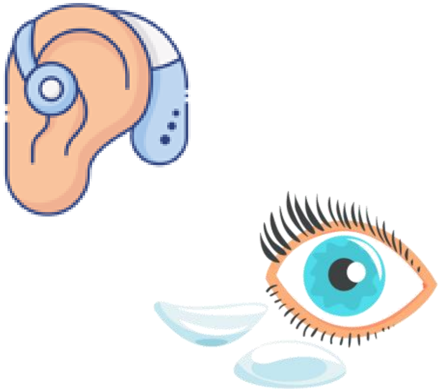
Risk class

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.

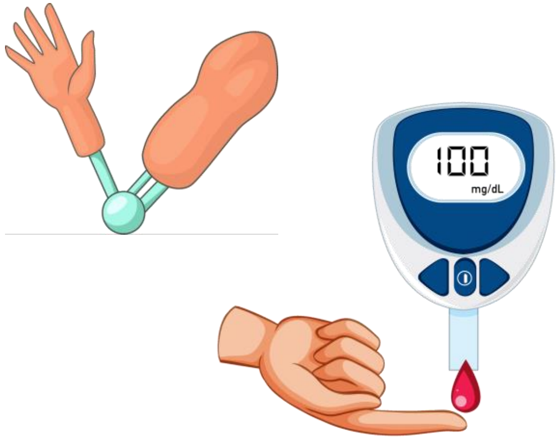
CLASS I
Low risk



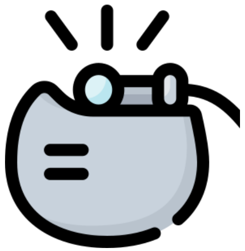
CLASS IIa
Medium risk



CLASS IIb
High risk



CLASS III
Highest risk



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,
<u>a security issue becomes a safety issue.</u>

Thanks for the attention!

Francesco Lestini

Contacts:
Pervasive Electromagnetic Lab,
Roma, Via del Politecnico 1

f.lestini97@gmail.com
francesco.lestini@uniroma2.it

CYBER4 HEALTH

Pervasive
Electromagnetics
Lab

Your opinion is important for us