Information and technology law course

LECTURE 19 – 25 NOVEMBER 2024

FEDERICA CASAROSA – 2024/2025

IoT applied to a wide range of aspects: not used medical because in terms of health, it is a general def. about elements associated to the state of an individual. We did not use to medical things on purpose.

If you have a device that can help you check the condition of a person without being there it would help you a lot. Another element could be control of devices remotely

Internet of Health Things

IoT

Ecosystem composed of

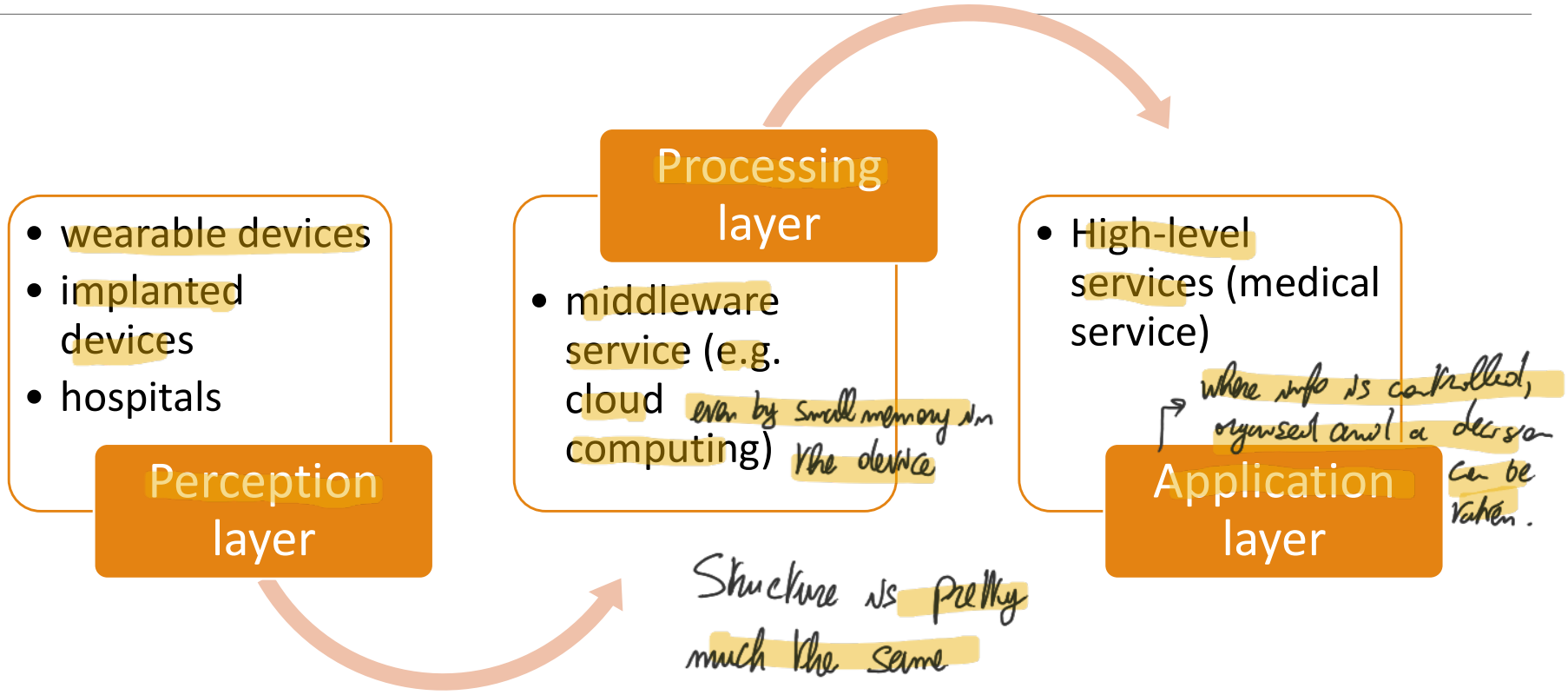
- objects connected to the network through sensors
- that interface with the physical world and interact with each other
- exchanging information on their status and the surrounding environment
- without the need for human intervention (↳ in some cases)

So def, not changed, applied to health.

- APPLIED TO THE HEALTH DEVICES

For example: think of wheelchairs: system could allow you to know where the wheelchairs are located. Or even the possibility to get them back autonomously. Or the possibility to have systems to check the amount of medicine still inside the bottle or devices that remind the patients of the time.

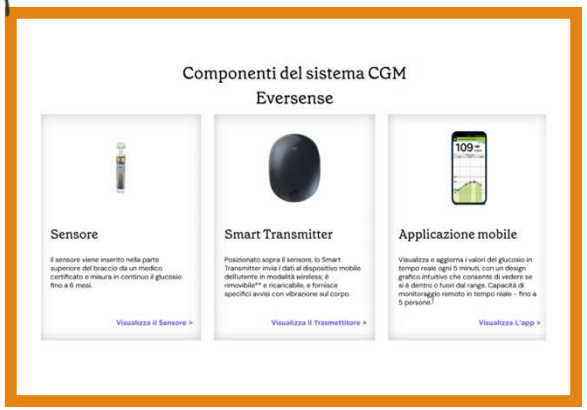
The structure of IoT technology in health

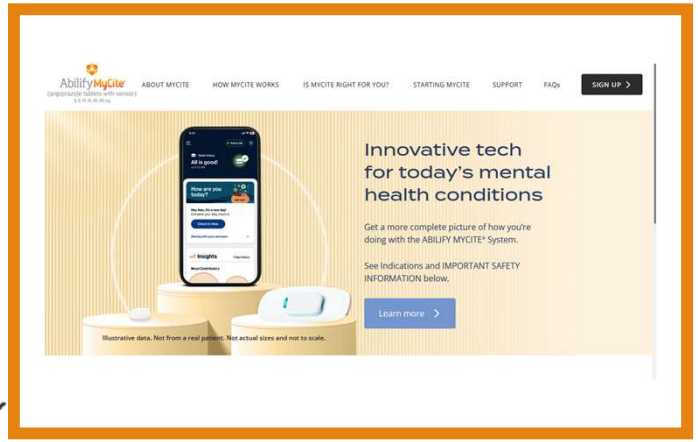


Examples of medical devices

System to check level of glucose in the blood, then smart transmitter etc.

to check if temperatures are correct in the room storing medicines. *





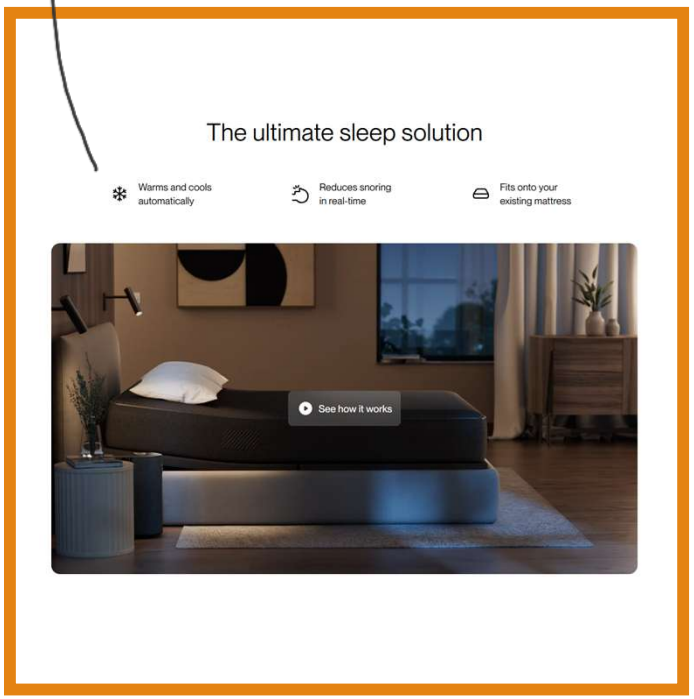
* Very important for the vaccines pills given when serum levels are perceived

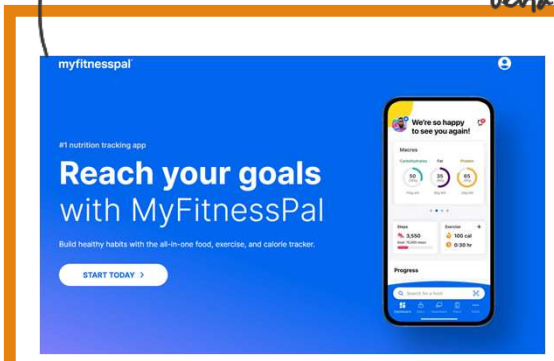
Smart Pillbox: recognise the time of opening and an alert of when to do something

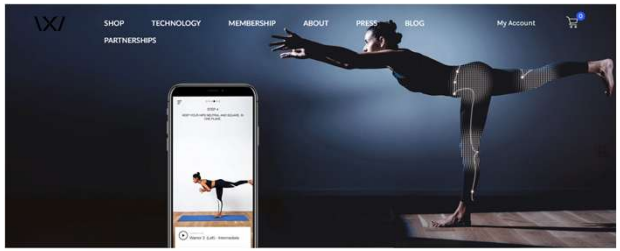
Examples of wellness devices

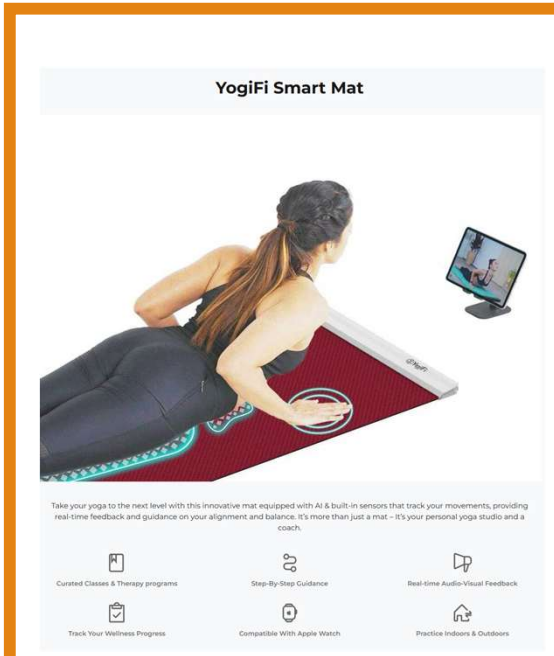
Not a medical condition related, but something health related.

App that registers your steps and gives info reacting to your behavior









In each of these cases, you have device that collect the info from environment, adapt to it and provide operations.

Think about an attack: the melanoma case (Benign, malign) we have to think about possibility to protect devices from the legal perspective.	Data protection	Cyber-security
General data protection regulation	√	√
Medical Device Regulation		√
Cyber resilience act		√

GDPR application

Processing of health data

- art. 4 (15) GDPR
  - data related to health are defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."
- Recital 35
  - health data cover the data subject's past, current or future health conditions.

- Lawful processing
  - art. 9 GDPR
    - Processing of special categories of data only in case of specific legal basis: consent by the data subject, data processing carried out to protect the vital interests of the data subject or another natural person when the data subject is physically or legally incapable of giving consent, data manifestly made public by the data subject, data processing aimed at preventive or occupational medicine and also data processing for reasons of public interest in the area of public health.

① Phys. or mental health: elements related to my physical and mental condition. They are related to a CURRENT SITUATION. ② Provision of services like prescription of glasses or drugs, even if I do not use them: they can reveal information about my health status. They are indirect elements.

(35) Goes even beyond: imagine a check for heart conditions because your parents have a certain condition. Think about genome research about genetically transmitted diseases: this info can be used to infer info about family, for ex.

③ Can a doctor or someone providing info for solutions for backpain use data? Yes.

GDPR application

Security requirements

- Art. 32 GDPR
  - data controller should "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" to protect personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage.

- What happens in case of violation?
- CNIL decision SAN-2022-009, 15 April 2022 :
  - French Data Protection Authority imposed an administrative fine of 1.5 million euros on a company dealing with medical data which failed to comply with Arts 28, 29, and 32 GDPR.
  - The security of personal data was not ensured, as numerous technical and organisational breaches in terms of security were found: lack of a specific procedure for data migration operations;[1] lack of encryption of personal data stored on the problematic server; no automatic deletion of data after migration to the other software;[2] no authentication required from the Internet to access the public area of the server; use of user accounts shared by several employees on the private area of the server;[3] lack of a procedure for monitoring and reporting security alerts on the server.

→ lot of cases instead of the org. were considered as breaches.

1. No control, encryption etc.

② Storage limitation,

③ Who has done what?

All of this is relevant for IoT too. Imagine migration of data from one cloud to another!

medical device: any instrument, appliance, implant, software intended by the manufacturer to be used by human beings for medical purposes

Medical Device Regulation application

Medical Devices Regulation 2017/745

- Art. 2(1) MDR

↳ Piece of leg. adopted in 2017. Reformulation to a previous directive

(1) ◦ A medical device is "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for the purpose of diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability; investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; and providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

◦ NB inclusion of 'software' among the types of medical devices, both stand-alone software and software connected to other software, and software offered as a service to another medical device.

Whatever can be a SW: even something that tells you to take medicines.
If it falls into the purposes listed, you have to go through steps of certification to have it usable

and you can get fines. If you are using your device for medical purposes you have to go through the process of certification. The list is very wide, BTW. (3)

We didn't have enough harmonization basically. This was specifically looking at medical devices. Basically, used from patient by doctors, a medical device should go through meticulously checked steps: you want a device not only on the market, you have to have critical tools to show that your device has good impact on the health of the people etc. This process applies for ①

③ Ex: the sw of theses could fall under the umbrella defined here. Alleviation and treatment of the disease could be implemented. Yet is not easy!
For ex. social robots for elderly people to keep elders interactive. Does this fall here? Age is not a disease! You have a device collecting info about someone and provides treatment but not for a disease! Here these specifications would not be applicable.

Medical Device Regulation application

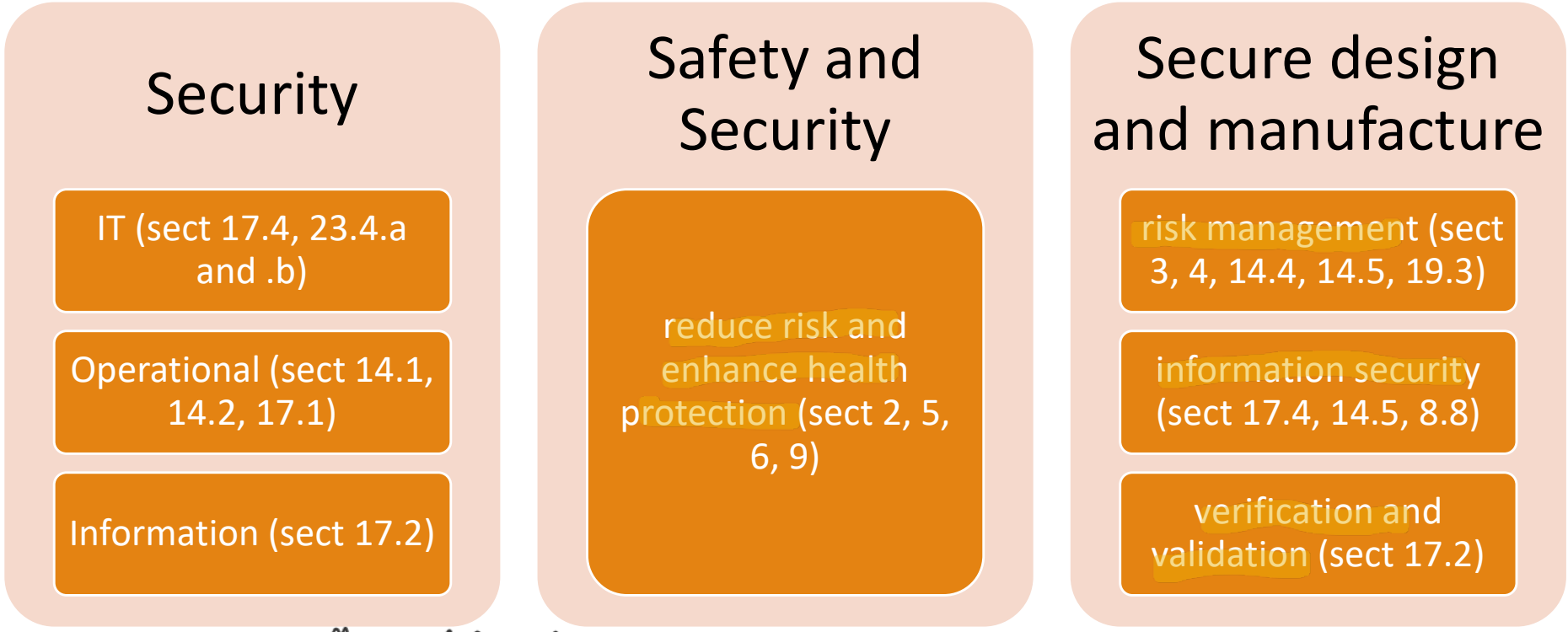
Medical v wellness devices/software

- If the purpose is among the ones listed, the device/software qualifies as a medical device
  - art 2 (12) MDR : the purpose is indicated by the manufacturer. Therefore, it is up to the manufacturer to provide information about the device's purpose on the label, in the instructions for use or in promotional or sales materials or statements.
  - BUT IoT devices that do not have a medical purpose are not subject to the MDR. However, they may still be used in medicine as they collect health-related data.

IOMT

- certification procedure requiring compliance with a minimum essential quality and safety criteria defined in Annex I MDR.

Medical Device Regulation application



Security not really qualified about CS. We can distinguish between operational security, information security, information technology security are the requirements. All these elements don't speak about CS but CS fields works some, hidden behind these requirements.

This is still before the product is put on the market.

Okay; now you received your certification. What now? Check what happens in the future.

Medical Device Regulation application

Notification procedure

not a security incident: what is a serious incident?

Art. 87 MDR : In case of a serious incident, the manufacturer must report the incident to the relevant competent authority.

Art. 2 (65) MDR, a serious incident is "any incident that directly or indirectly led, might have led, or might lead to any of the following:

- the death of a patient, user or other person, ①
- the temporary or permanent serious deterioration of a patient's, user's or other person's state of health,
- a serious public health threat.

Timeline:

- 2 days after the manufacturer becomes aware in case of a serious public health threat
- 10 days after the causal relationship between the device and serious incident is established/suspected in case of death or a severe unanticipated deterioration in a person's state of health
- 15 days after the causal relationship between the device and serious incident is established/suspected to any other serious incident.

① Imagine a pacemaker attack: this can be a serious incident. CS incidents can still fall under the umbrella of serious incident.

Why such long periods: not easy to become aware and connect medical device with serious incident. Security incident is easier. Remember that health is also a sector for NIS 2.

Medical Device Regulation application

Manufacturers must

- conduct investigations as soon as they are informed that a serious incident has occurred
- take corrective actions for medical or technical reasons to prevent or reduce the risk of a serious incident, i.e., field safety corrective actions (FSCA)
  - the return of a device to the supplier or a recall, a device exchange, a device modification, retrofit by the purchaser of manufacturer's modification or design change, a device destruction, advice given by the manufacturer regarding the use of the device, recommended inspections/examination by the device user, changes of software/firmware in the device, including device update.
- As soon as the manufacturer decides to implement any of these measures, the device users should be informed through a field safety notice (FSN) to ensure that required actions are followed and completed in a timely manner.

Interplay between GDPR and MDR

collecting personal data

Medical IoT should comply at the same time with the GDPR and the MDR requirements. Do the two authority speak to each other? ①

- Are the national notification bodies in charge of verifying compliance with MDR requirements also asked to verify compliance with GDPR?
- To what extent, for instance, is the DPIA carried out by the manufacturer as a data controller sufficient to demonstrate the security measures provided in the MDR? Regarding security of data, for example? Open questions.

① If I have a notif I take for granted that I am compliant with the GDPR. In theory the nmb will take a look, but it's possible that that's not enough.

Imagine Social care robots: not used to treat a disease. But is there anything applicable for security?
Yes, CRA.

CRA application

↑ all products with digital elements fall under the definition.

IoHT are products with digital elements

- Art. 2(68) CRA "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."

CRA's scope of application does not cover products with digital elements that are covered by the definition of medical devices

- IoMT subject to the MDR security and safety requirements
- IoHT subject to the CRA requirements for cybersecurity

Before 2022, security was up to the manufacturer!

CRA application

Art. 13 CRA

- Before they are put on the market, products with digital elements must be designed, developed and manufactured in such a way as to ensure an appropriate level of cybersecurity.
- Products must be delivered without known exploitable vulnerabilities and deployed in a secure default configuration.
- Annex 1 – Security and vulnerability handling equirements

Notification

- Art. 14 CRA
- Manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.
  - a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it
  - (b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability
  - (c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available

Let's take IoMT:

IoMT —— GDPR
MDR

What if there's a problem? I have to check if there's a data breach or if it is a serious incident. It is probable that the two things overlap [determination of health?]. But what if it is? As a manufacturer, I have to notify the DPA about the data breach in 72 hours and in the worst case within 48 h to the Medical Authority. And I need different information too. This is tricky for a manufacturer. I don't even have confirmation of compliance with GDPR.

IoHT → CRA
GDPR

I can have data breach (2), and incident or vulnerability exploitation. It is frequent to have an overlap. Here we need the notification to the DPA (72hrs) and to the CSIRT + ENISA in 24 hrs. But even here, tricky. All these problems emerge with parallel legislations adopted in different times.

Open issues

- Coordination between horizontal legislation and sector-specific ones
  - Distinction between medical and health devices
  - Generic standards in CRA
- Notification overload
  - No overlapping timeline
  - Different authorities
  - different content

GDPR

MDR

The requirements are quite sectorial

CRA: requirements are not adapted to sector specific products! We could have standards in the future but this would make the sys more complex.

Same incident, but different authorities looking at different perspectives.