SoteDigi

“Medical device regulation supports cyber resilience of the smart hospital”

Finnish Internet Industrial Forum
“Digital trust and security” 14.2.2019

SoteDigi – in brief

National company for social and health care digitalization, founded 2017 by Finnish government

Owned 100 % by government, in the future also by regional governments

Appr. 30 employees (February 2019), growing up to 50 by the end of the year

Three main focuses in project portfolio

- digital services for citizens
- business intelligence
- integrations

Working in collaboration and co-operation with

- regional governments
- national organizations (f.ex Kela - Social insurance institution of Finland, and THL (National institute for health and welfare)

SoteDigi

Jenni Siermala

Education:

Master degree information process science 2015

I am Doctor Candite. My thesis topic consern security and safety in telemedicine

Work:

I have worked Oulu univercity hospital for ten years

Now I am *chief information security officer (CISO)* at SoteDigi

SoteDigi

What if…

The patient receives a insulin pump.

The patient's strength rises and his quality of life improves because he does not need to monitor the insulin values himself.

The patient monitor from a mobile application the insulin level long-term trend.

Suddenly patient's condition collapses and he dies.

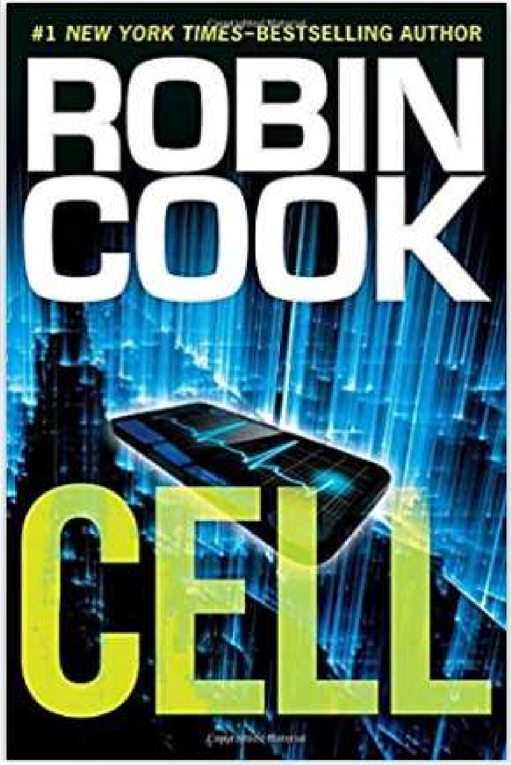
It turns out: in a routine check the patient has been found the incurable cancer.

After the cause of death studies and the presence of an emergency doctor

It is evident that insurance company has hacked the patient's insulin pump to give the drain command.

SoteDigi

This is the story ..



The New York Times–bestselling author and master of the medical thriller

SoteDigi

Smart Hospital

enisa

Smart Hospitals

Security and Resilience for Smart Health Service and Infrastructures

NOVEMBER 2016

ENISA: Cyber security and resilience for Smart Hospitals

Published november 24,2016

” The notion of smart hospitals is introduced when Internet of Things (IoT) components are supporting core functions of a hospital.”

report was developed using a combination of desktop research as well as information from interviews with key stakeholders.

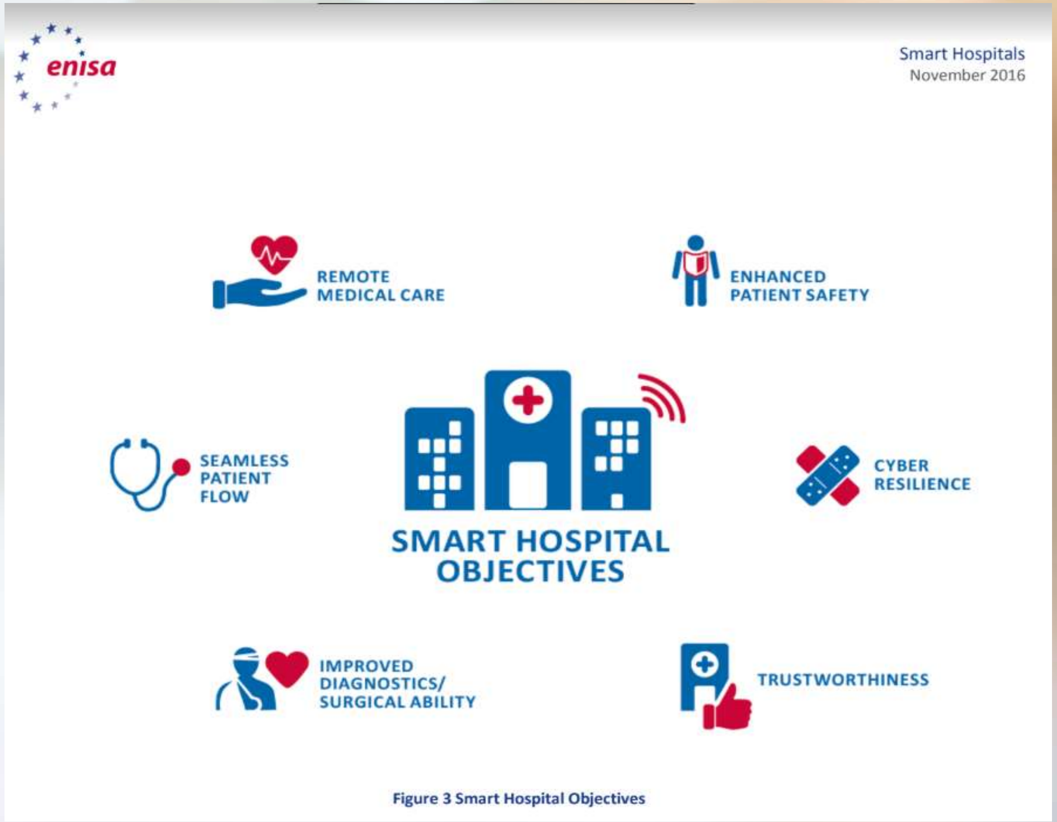
The document analysis focuses on scientific, as well as industry and policy material, related to information security in smart hospitals.

SoteDigi

Smart hospital

"A smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities".

SoteDigi



enisa

Smart Hospitals
November 2016

REMOTE MEDICAL CARE

ENHANCED PATIENT SAFETY

SEAMLESS PATIENT FLOW

SMART HOSPITAL OBJECTIVES

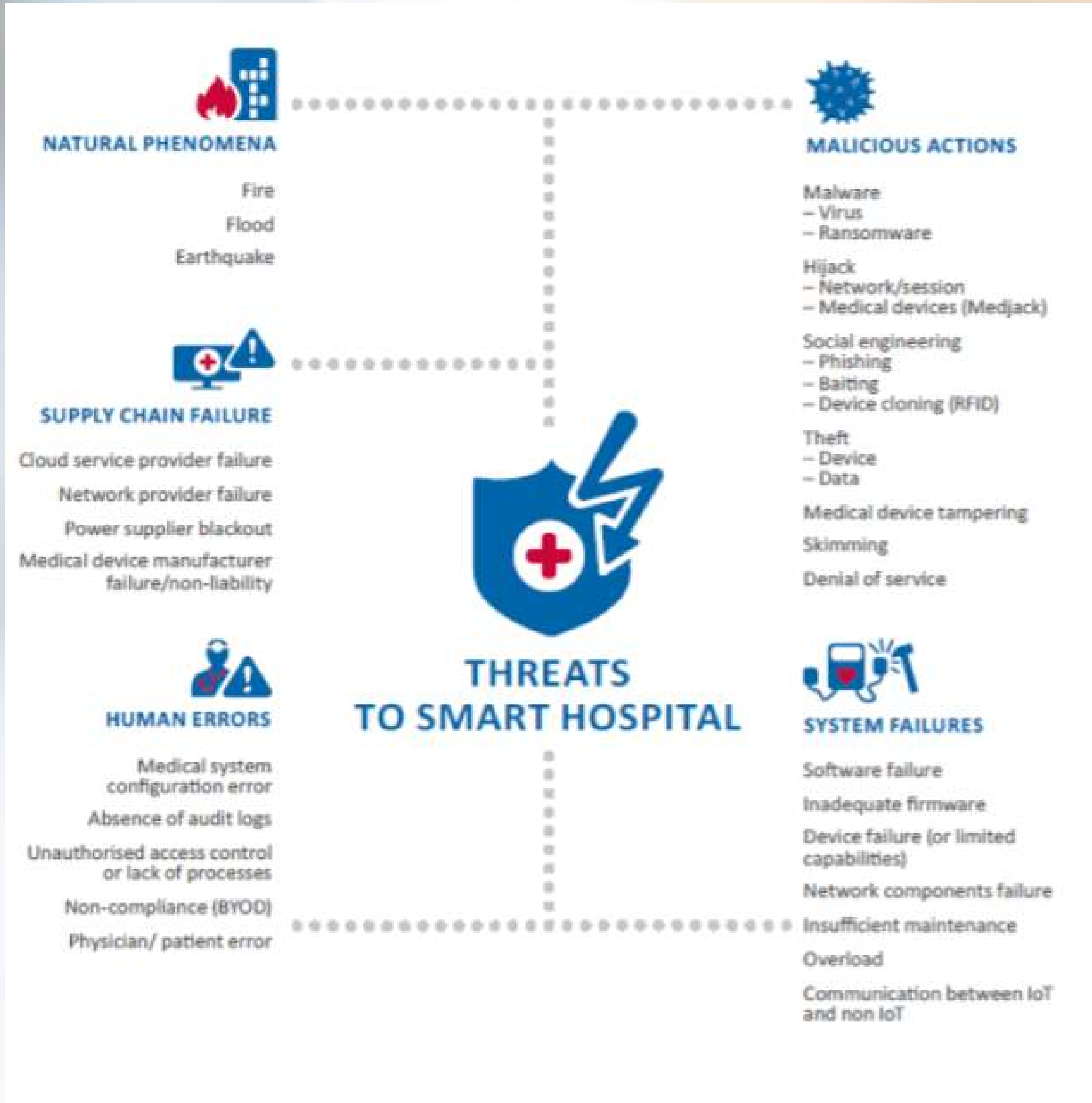
CYBER RESILIENCE

IMPROVED DIAGNOSTICS/ SURGICAL ABILITY

TRUSTWORTHINESS

Figure 3 Smart Hospital Objectives

SoteDigi



THREATS TO SMART HOSPITAL

NATURAL PHENOMENA

- Fire
- Flood
- Earthquake

SUPPLY CHAIN FAILURE

- Cloud service provider failure
- Network provider failure
- Power supplier blackout
- Medical device manufacturer failure/non-liability

HUMAN ERRORS

- Medical system configuration error
- Absence of audit logs
- Unauthorised access control or lack of processes
- Non-compliance (BYOD)
- Physician/ patient error

MALICIOUS ACTIONS

- Malware
  - Virus
  - Ransomware
- Hijack
  - Network/session
  - Medical devices (Medjack)
- Social engineering
  - Phishing
  - Baiting
  - Device cloning (RFID)
- Theft
  - Device
  - Data
- Medical device tampering
- Skimming
- Denial of service

SYSTEM FAILURES

- Software failure
- Inadequate firmware
- Device failure (or limited capabilities)
- Network components failure
- Insufficient maintenance
- Overload
- Communication between IoT and non IoT

Figure 6 Threats to smart hospitals

SoteDigi

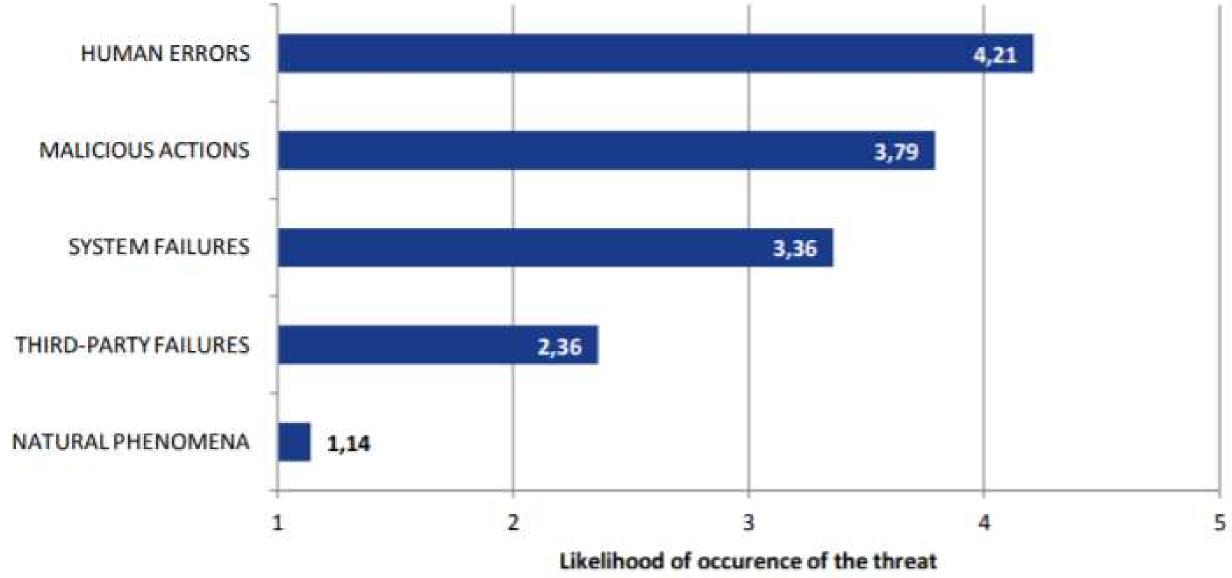
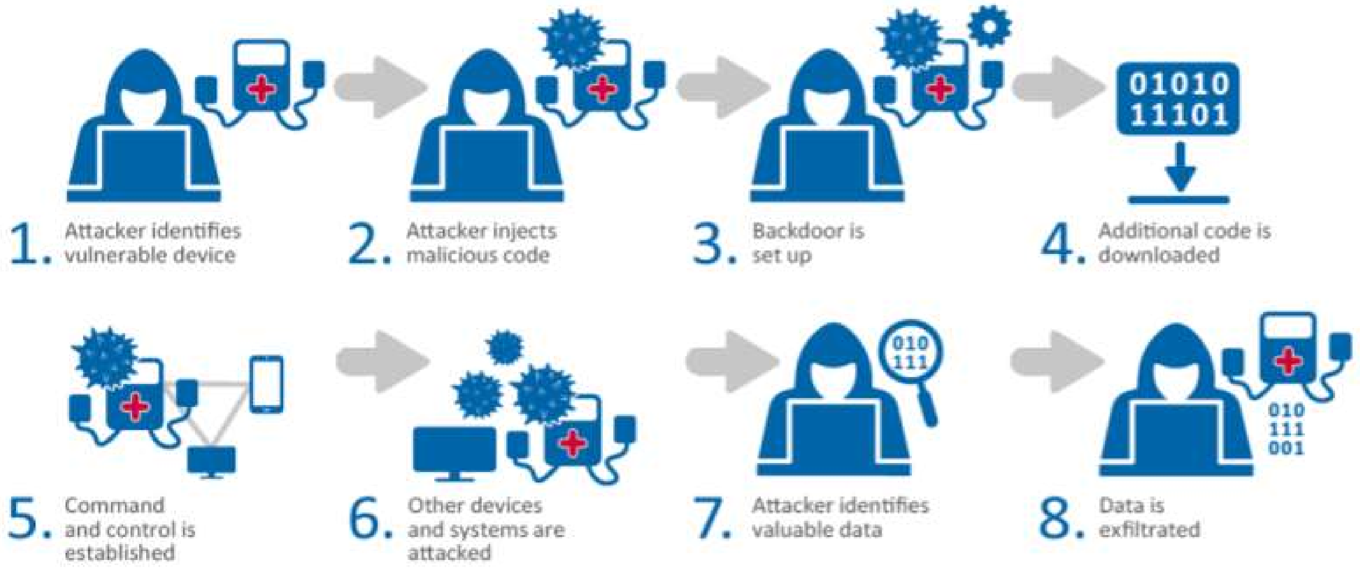


Figure 7 Likelihood of occurrence of threats

ATTACK SCENARIO 2 - TAMPERING WITH MEDICAL DEVICE



1. Attacker identifies vulnerable device

2. Attacker injects malicious code

3. Backdoor is set up

4. Additional code is downloaded

5. Command and control is established

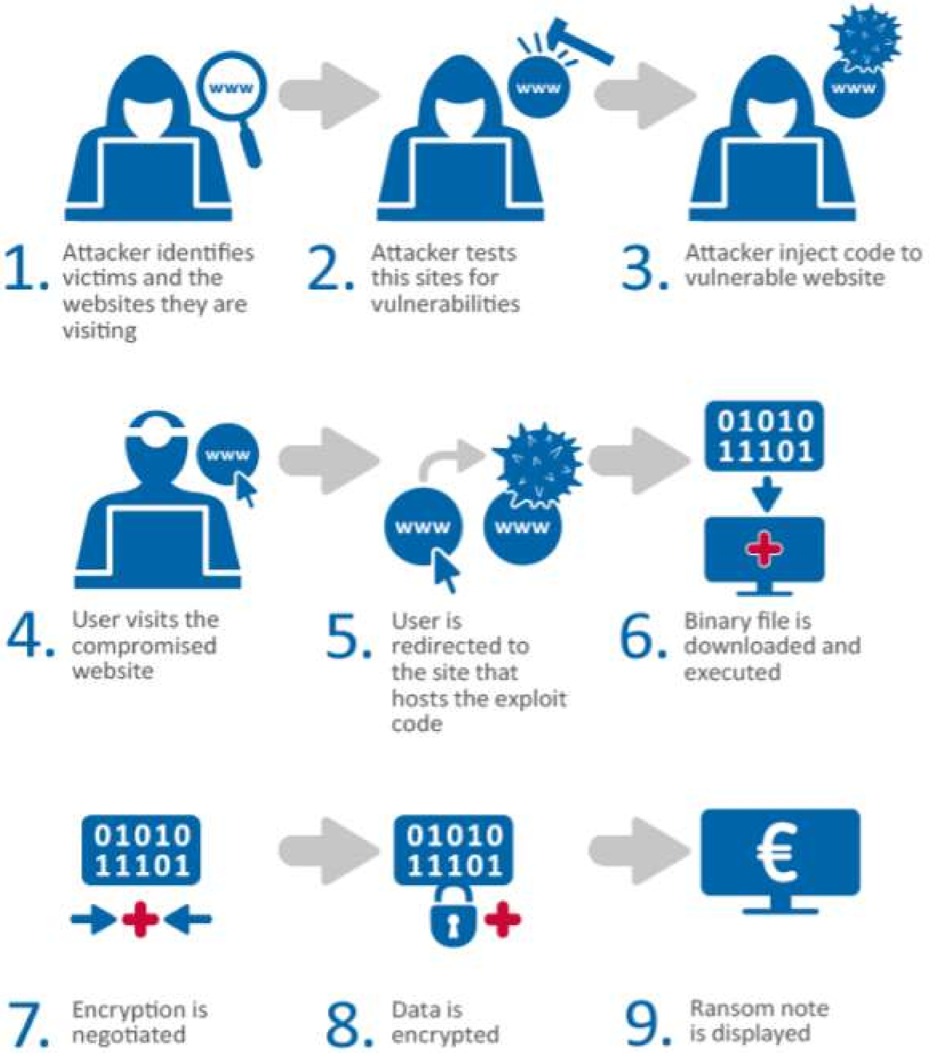
6. Other devices and systems are attacked

7. Attacker identifies valuable data

8. Data is exfiltrated

Figure 11 Tampering with medical devices

ATTACK SCENARIO 4 – RANSOMWARE



1. Attacker identifies victims and the websites they are visiting

2. Attacker tests this sites for vulnerabilities

3. Attacker inject code to vulnerable website

4. User visits the compromised website

5. User is redirected to the site that hosts the exploit code

6. Binary file is downloaded and executed

7. Encryption is negotiated

8. Data is encrypted

9. Ransom note is displayed

Figure 13 Ransomware attack on hospital information system

Regulation

MDD

Medical Devices Directive 93/42/EEC of 14 June 1993

MDR

Medical Device Regulation is a new Regulation (EU) 2017/745 of the European Parliament

The regulation will enter into force after a transitional period 20.5.2020

SoteDigi

What is Medical Device?

Means an equipment, instrument, software, implant, reagent, material or other accessory intended by the manufacturer to be used by humans, either alone or in combination, for the following medical purposes:

- diagnosis, prevention, anticipation, prognosis, monitoring, treatment or alleviation of the disease,
- diagnosis, alleviation or compensation of injury or disability,
- examining, replacing or modifying anatomy or physiological or pathological function or condition,
- obtaining information from samples taken from the human body, including the donation of organs, blood and tissues, by means of studies performed outside the human body

SoteDigi

Examples

- Patient Information Systems / Electronic Health Information Systems
- Symptom estimation software
- Imaging systems
- Patient monitoring monitors
- Measuring sensors
- ECG electrode
- Blood pressure monitors with accessories
- Artificial intelligence applications for medical use

SoteDigi

MDR – The Manufacturer

- The medical device must be registered before use in Finland Valvira
- The manufacturer of the medical device must have an appropriate quality system (**ISO 13485**)
- Notified body grant the medical device accept CE marked
- The device is classified in the Medical Device Regulation based on the risk generated by the device
- The manufacturer must monitor the operation of the device and report to the authorities
- The manufacturer must have processes for handling incidents and advisory reports
- The safety of the device is answered throughout the life cycle

SoteDigi

MDR - Patient safety

- The manufacturer must determine the manufacturing of the medical device the necessary and sufficient processes to ensure patient safety
- The manufacturer must define processes for identifying patient risks and to remove them
- The manufacturer must take the specified measures to prevent it potential hazard or remove (eg by repair) dangerous device on the market (incident occurred)
- Clinical evaluation is mandatory for all medical devices and for that related clinical research is mandatory for high-risk devices
- Ensure the device is fit for it purpose and patient safety

SoteDigi

MDR – Product risk management

- Product risk management is intended to analyze the products in the product security risks and make a plan for these risks to remove
- The product risk management process covers the entire product lifecycle
- The process also includes product risks throughout the product lifecycle evaluation planning and risk summary
- The safety of medical devices must be ensured before the product is placed on the market and safety must be monitored throughout the product's lifecycle

SoteDigi

What is even better?

- MDD did not allow any changes after the medical device standardization

→ Not even update computer if it was included

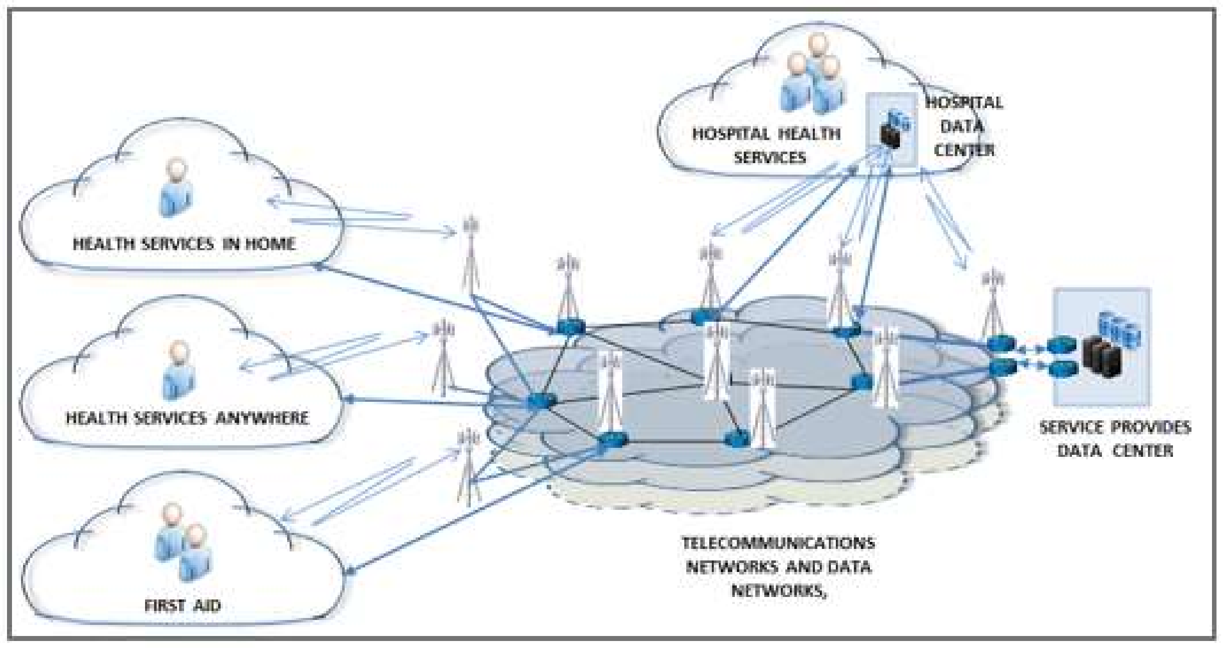
→Lifecycle safety did not actualize

- MDR requires the manufacturer accept the responsibility of the device

→Not the smart hospital

SoteDigi

What then..



SoteDigi

Thank you
Contact:
jenni.siermala@sotedigi.fi

SoteDigi