Panacea

People-centric cybersecurity in healthcare

Biometrics in the Panacea project

January 2019-December2021

EAB Sept 2020

Aghiles ADJAZ, Claude BAUZOU, Emmanouil SPANAKIS

IDEMIA **FORTH**

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

Outline

- An introduction to PANACEA → Claude
- The “IMP H2M” solution → Aghiles
- Contribution to TR 21419, Biometrics in Healthcare → Manolis

An introduction to PANACEA

Claude BAUZOU

IDEMIA

Panacea
People-centric cybersecurity in healthcare

Panacearesearch.eu, in a nutshell

What

A Research & Innovation Action (RIA) dealing with cybersecurity in the healthcare sector

Objectives

- Deliver an **innovative cybersecurity toolkit**, providing a holistic approach for Health Care Institutions
- Combine **technical** (SW platforms for dynamic risk assessment, secure information sharing & security-by-design) and **non-technical** (procedures, governance models, people behaviour tools) elements.

When

From January 2019 up to December 2021

36 Months of Activity

Who

A team of 80+ academics & professionals: 15 partners from 7 EU Countries

PANACEA Research will help the healthcare sector respond more swiftly to the risks of a complex threat landscape while fostering positive behavioural changes in order to tackle cyber threats and protect healthcare services and patients.

Panacea
People-centric cybersecurity in healthcare

The Consortium

Use Cases

Project Coordinator:

Università Cattolica del Sacro Cuore

Fondazione Policlinico Gemelli

7th Health Region of Crete

HSE South / South West Hospital Group Ireland

Large Enterprises

AON

IDEMIA

RINA Consulting

SMEs

Irish Centre for Emergency Management

Innovation Sprint

RHEA

Stelar

Trust-IT Services

Research & Academia

UniRome

UNAN

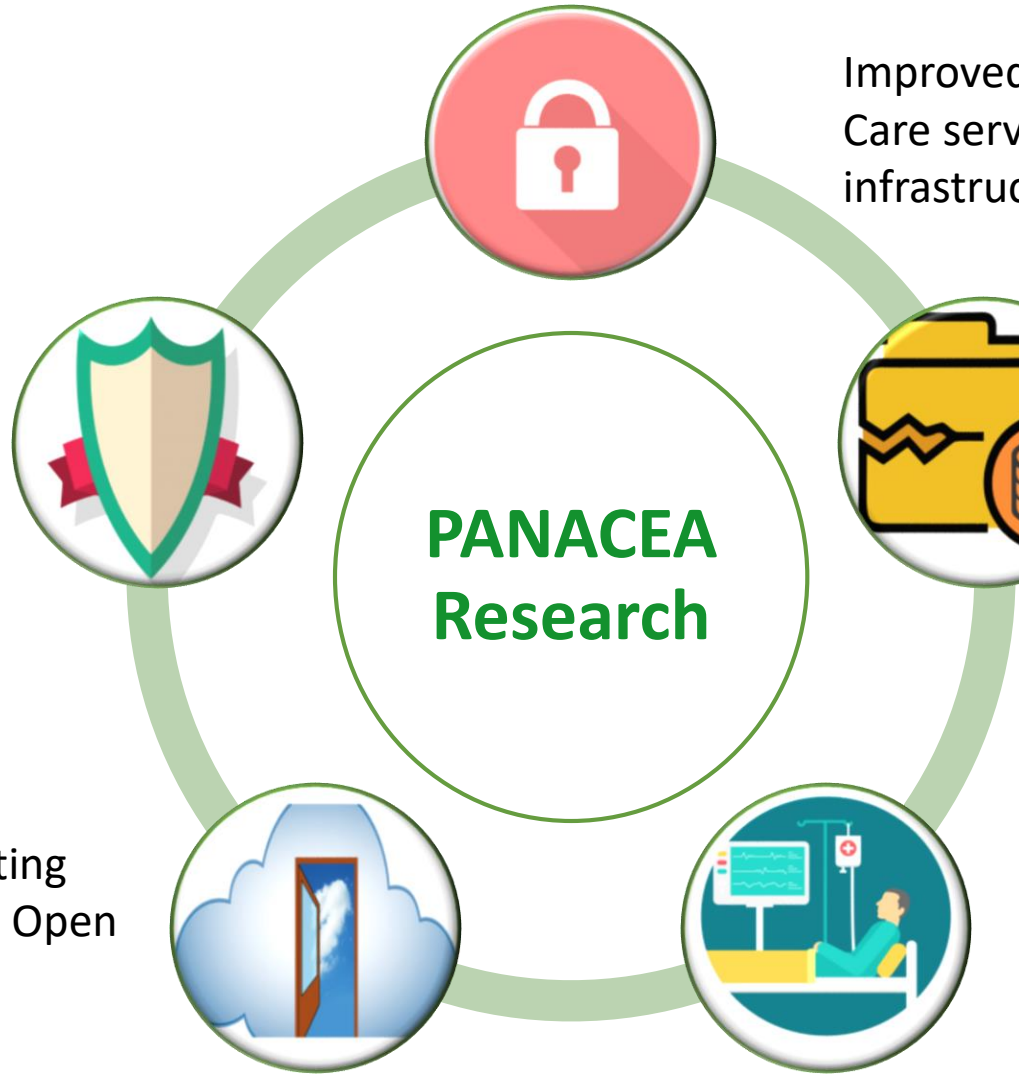
FORTH

Challenges for Healthcare Cybersecurity

- HC providers share **attractiveness** for cybercrime because
  - healthcare is a rich source of valuable data
  - Their defences are weak.
- Key reasons of **weakness** include:
  - **Dynamic Complexity**: continuously changing multiplicity of connected end-points, different interconnected systems; increasing digitalization of patient data.
  - **Barriers to the adoption of security solutions**: skill shortage, performance concerns, lack of budget, lack of organisational buy-in.
  - **Human error**: because healthcare staff are overwhelmed by their professional workload (rush is a constant of their work environment).

Panacea
People-centric cybersecurity in healthcare

What's the impact?



Improved security of Health and Care services, data and infrastructures

Less risk of data privacy breaches caused by cyberattacks

Increased patient trust and safety

Cross-cutting priorities: Open Science

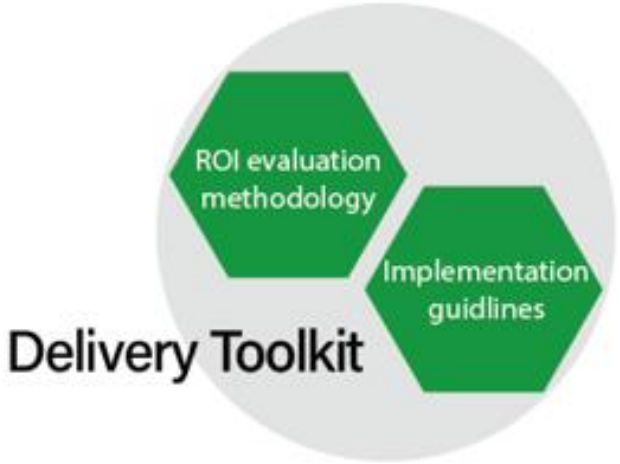
Supporting Standardisation Efforts

Developing a complete and sustainable set of products & and services offering that will significantly expand the opportunities at reach for healthcare organisations across sizes, organisational models and ICT infrastructures.

Panacea toolkit

Technical tools

Deliver an **innovative cybersecurity toolkit**, providing a holistic approach for Health Care Institutions

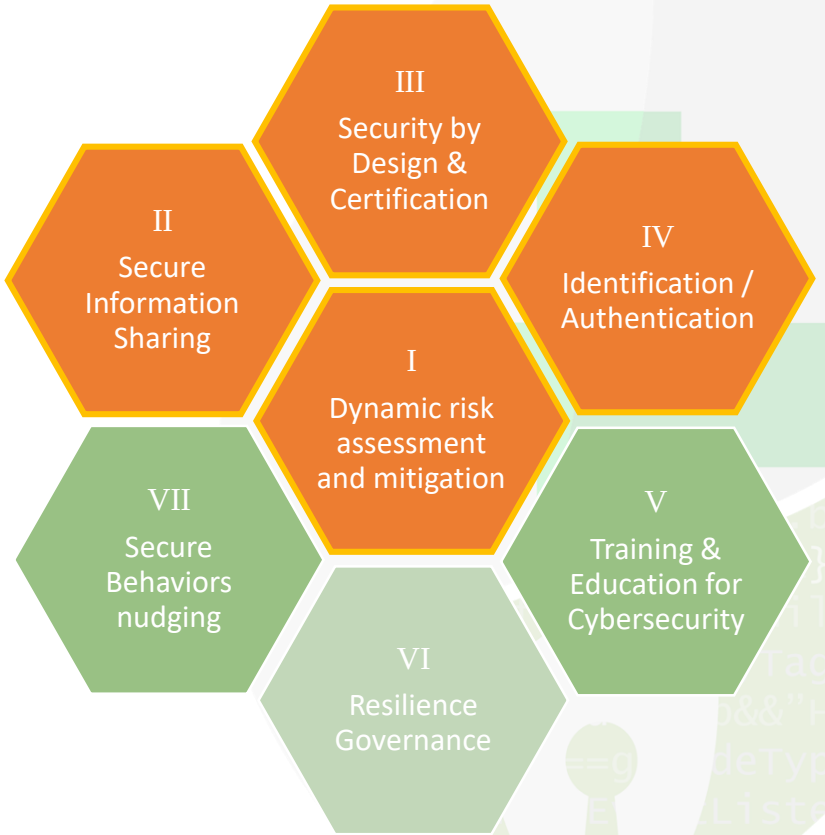


Organizational tools

Technical Tools in PANACEA

- **Dynamic Risk Assessment Platform** – DRMP - (RHEA, UNIROMA, RINA)
- **Secure Information Sharing Platform** – SISP - (RHEA, with scientific support from FORTH)
- **Secure Design Support Platform** – SDSP- (RHEA)
- **Compliance Support Tool** –CST- (RINA)
- **Identity Management Platform** –IMP-
  - Human to Machine IMP (IDEMIA)
  - Machine to Machine IMP (iSPRINT)

- **Challenge**: many tools, limited effort and time, multiple different organizations involved, multiple topics



More details on the IMP-M2M

- M2M means secure communication between Medical devices / systems: they must be secure…
- With the development of medical IoT, this is of extreme importance because the threat could be on patient life

More details on IMP-H2M

- We focused on access control
  - Logical
  - Within the hospital, for hospital personnel
- For computers
- For medical devices

More details on IMP-H2M

- IMP-H2M will be validated in four use cases:
  - Access to work-stations used in a very busy Laboratory, in Gemelli Hospital (Italy)
  - Access to Medical Device used in a clinical ward by many nurses, in Gemelli Hospital
  - Access to an application used to share data
    - in a health region, between staff located in different Hospitals/Local Diagnostic Centers/General Practitioners, in the 7th Heath Region of Crete
    - between staff located in Gemelli Hospital (Italy) and in South South-West Hospital Group (Ireland)

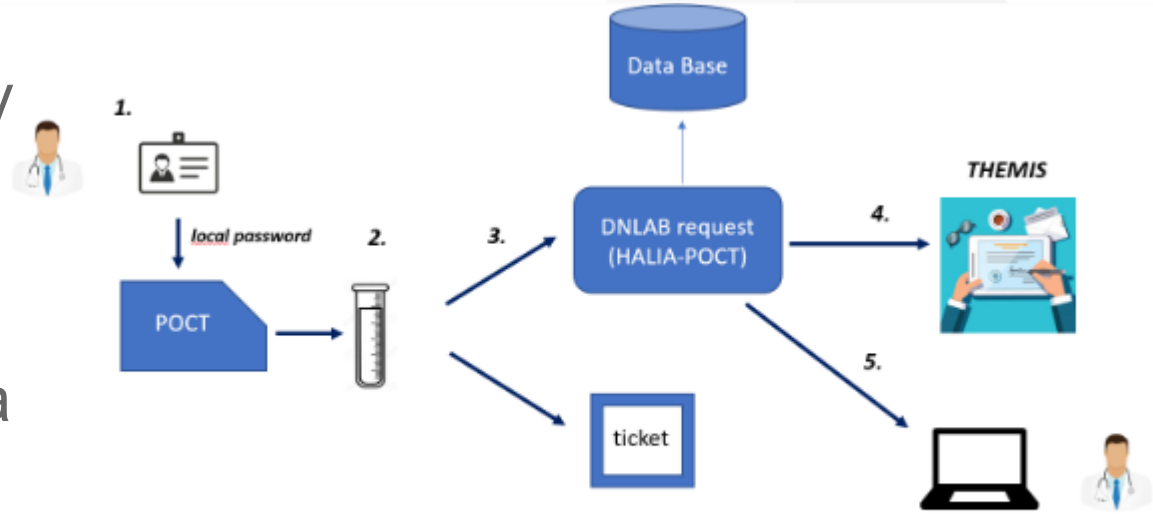


Figure 7-6 Urgent analysis process

Panacea
People-centric cybersecurity in healthcare

If you are interested…

www.panacearesearch.eu

Twitter: @H2020panacea
LinkedIn: /in/panacearesearch
YouTube: channel/UC5k4hx6IQiRd0nXNtWK_jMQ

Identity Management Platform – Human to Machine -

Aghiles ADJAZ

IDEMIA

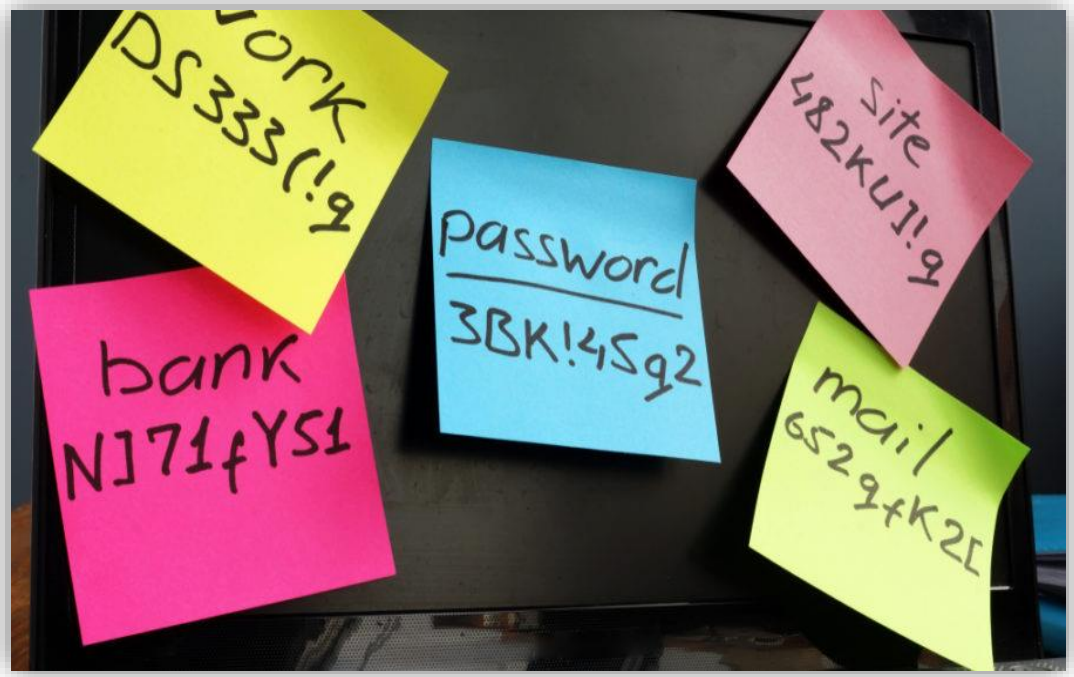
Today's solution

POCT-Point of Care Terminal

Based on :

- Login/Password authentication (1 factor)
- Windows Operating System (even for POCT)

In practice



- Credentials are written on post-it
- All people from the same team are using the same credentials (most of the time Manager's credentials)
- On some terminals authentication is disabled

Why ?

- Difficult to remember passwords
- Healthcare staff main concern is saving people not the security of data
- Writing login/password is time consuming

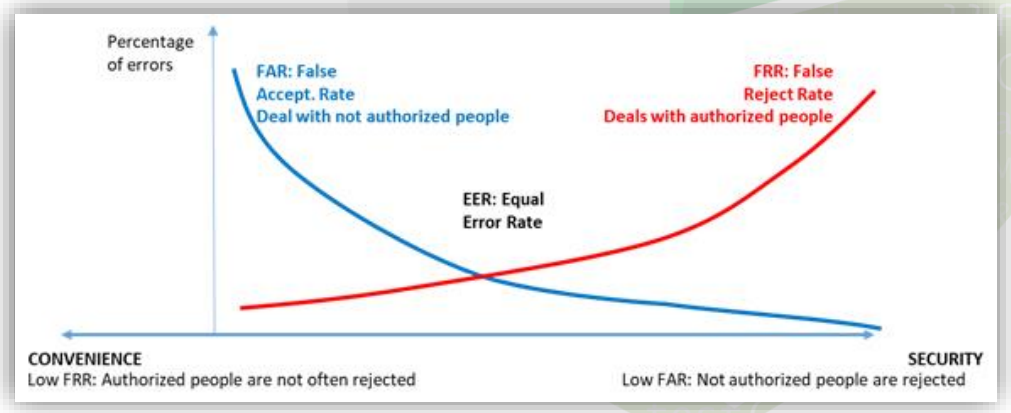
Why ?

→ Any proposed solution **MUST** be easy to use in order to be accepted by Healthcare staff (otherwise workarounds will always be found)

Research on authentication in the hospital

Authentication factors

- What I know (passwords)
  - Difficult to manage in a safe and reliable way
  - Takes some time to type...
  - "helper" like password management systems not suitable for shared equipment
- What I have (hardware token, such as badges, smartphones …)
  - Convenient
  - Not reliable enough on its own: must make sure to whom it belongs
- What I am (Biometrics)
  - Convenient
  - Not 100% reliable



Requirements

- Easy to use
- Secure
- Affordable
- Easy to integrate to the existing IT infrastructure
- GDPR Compliant

Requirements

- Easy to use (one click button)
- Secure
- Affordable
- Easy to integrate to the existing IT infrastructure
- GDPR Compliant

Requirements

- Easy to use (one click button)
- Secure (two authentication factors)
- Affordable
- Easy to integrate to the existing IT infrastructure
- GDPR Compliant

Which hardware, Which biometry

- Smartphone because it is a hardware that users carry always with them, provides a camera for face acquisition and BLE for transparent data transmission

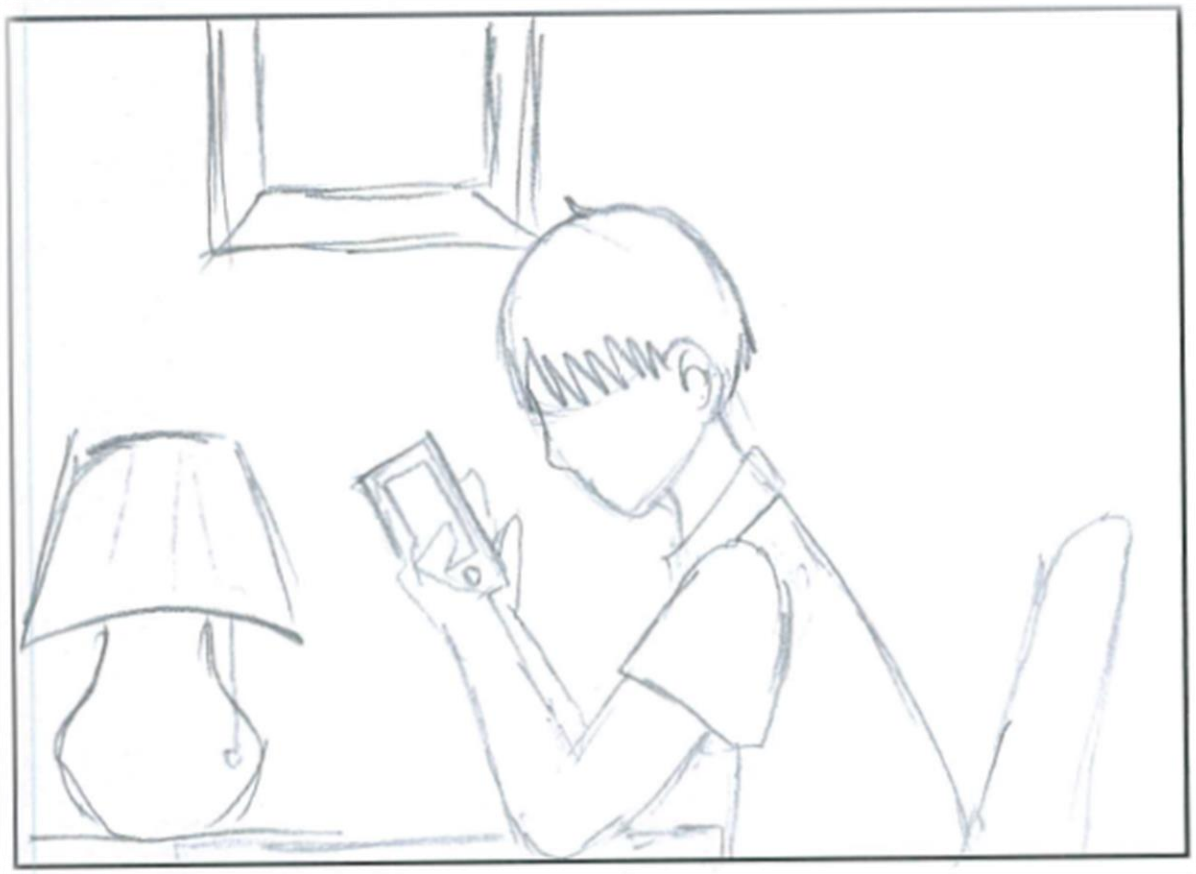
- Face because it is contactless, user-friendly, does not require special acquisition device

Voice	Iris	Face	Finger	Behavioral
Unsuitable in some environment (IRM machines…) Difficult to avoid recording other people (privacy) Not suitable for fast access control	Need specific device for acquisition	user-friendly, does not require special acquisition device	Not suitable when gloves are worn and need a specific device	Not suitable for fast access control

Requirements

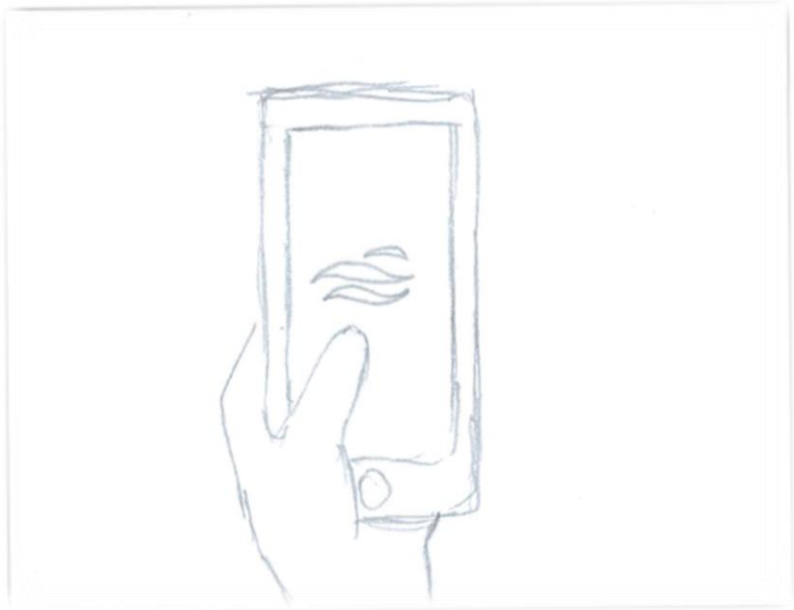
- Easy to use (one click button)
- Secure (two authentication factors)
- Affordable (smartphones, existing camera…)
- Easy to integrate to the existing IT infrastructure (software update on workstations)
- GDPR Compliant (user consent, decentralized biometric DB)

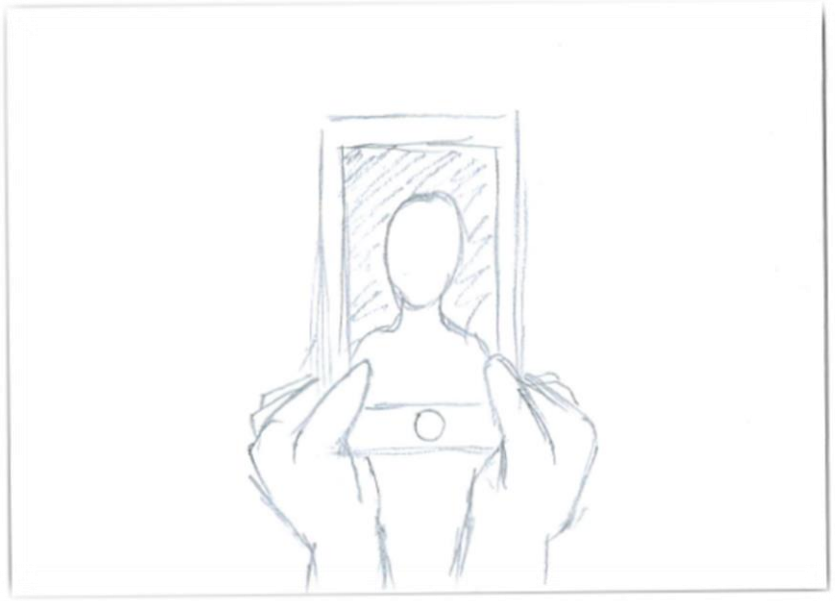
Storyboard



- User downloads the Panacea application

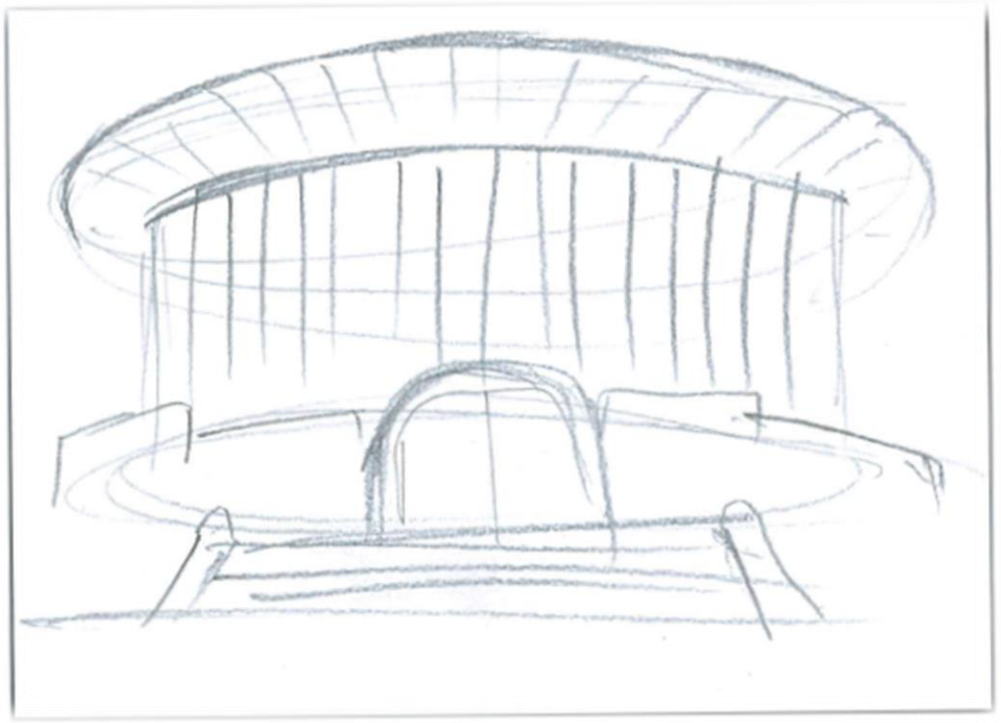
Storyboard





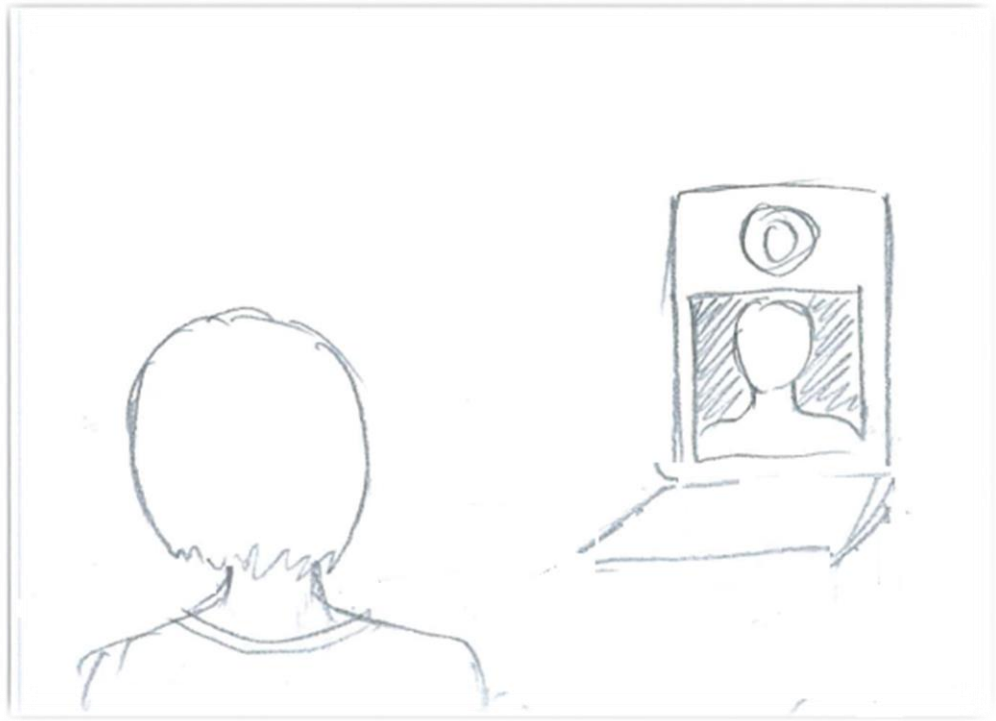
- User opens the Panacea application and registers himself

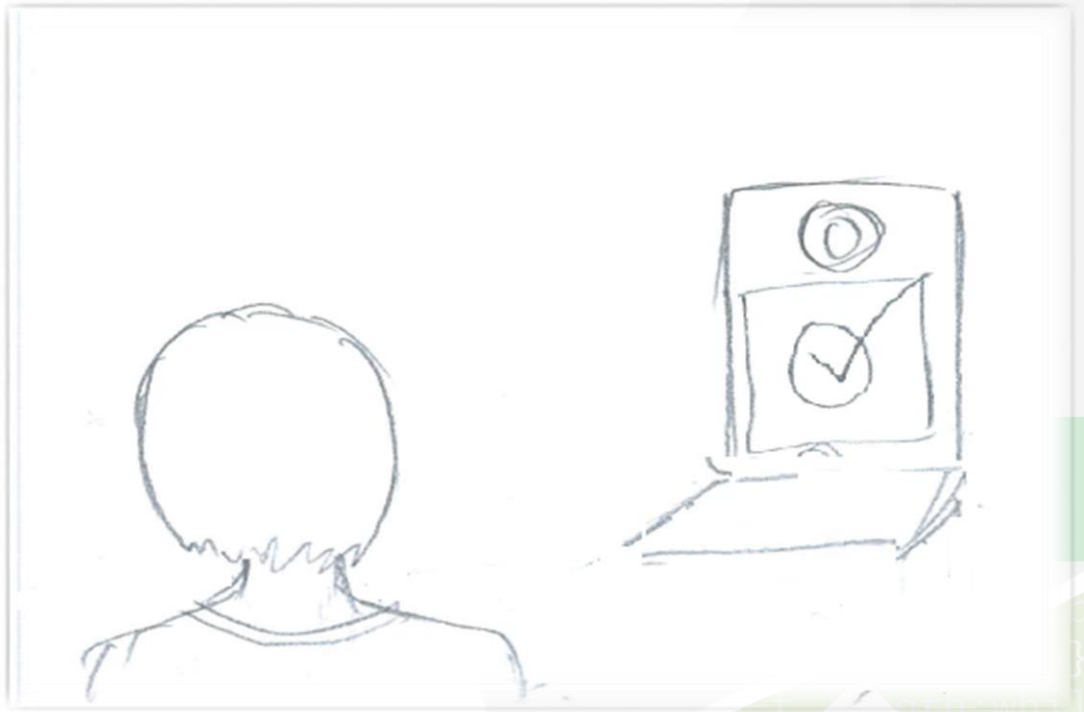
Storyboard



- User can go to work, keeping his smartphone always in his pocket

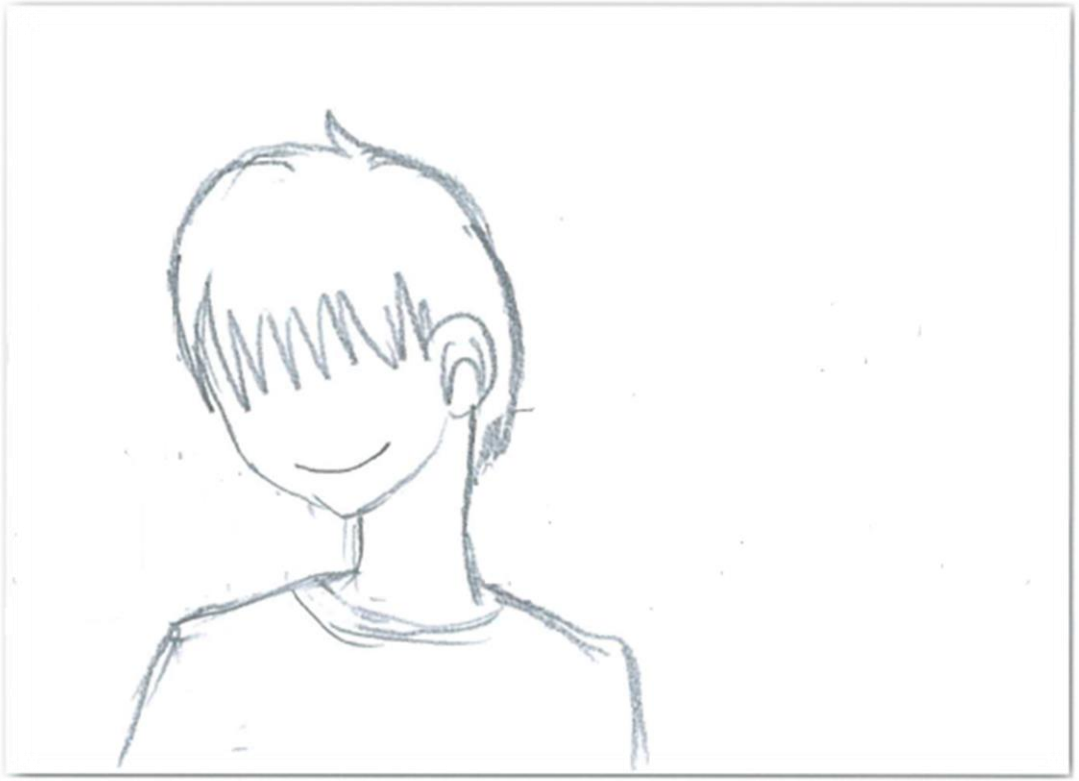
Storyboard





- User authenticates into the medical device using his biometry

Storyboard



- User is happy with the Panacea experience

Video

Panacea Video

NIST FRVT 1:1


1
ORIGINAL
IMAGE
2
WIDE,
HIGH
COVERAGE
3
WIDE,
MEDIUM
COVERAGE

NIST FRVT 1:1 Performances

Ref without mask, search with a mask

Algorithm	VISABORDER Photos FNMR @ FMR ≤ 0.00001 (NOT MASKED)	VISABORDER Photos FNMR@FMR ≤ 0.00001 (MASKED PROBE) lightblue, wide, medium coverage	Submission Date
deepglint-002	0.0039[9]	0.0237[1]	2019-11-15
paravision-004	0.0088[48]	0.0281[2]	2019-12-11
visionlabs-009	0.0028[1]	0.0355[3]	2020-07-27
iqface-002	0.0086[46]	0.0445[4]	2020-07-30
pensees-001	0.0106[60]	0.0461[5]	2020-08-17
vocord-008	0.0038[7]	0.0500[6]	2020-01-31
idemia-006	0.0048[17]	0.0539[7]	2020-07-06

Performance comparison with previous versions

Algorithm	VISABORDER Photos FNMR @ FMR ≤ 0.00001 (NOT MASKED)	VISABORDER Photos FNMR@FMR ≤ 0.00001 (MASKED PROBE) lightblue, wide, medium coverage	Submission Date
idemia-006	0.0048[17]	0.0539[7]	2020-07-06
idemia-005	0.0111[65]	0.6469[95]	2019-10-11

FNMR values are reported at a fixed threshold calibrated to give FMR = 0.00001 on unmasked images. Algorithms in black were submitted prior to mid-March 2020, and algorithms in blue were submitted thereafter.

Conclusion

- Resolve credential sharing issues in hospitals
- Two authentication factors (What I have and What I am)
- Frictionless & easy solution thanks to the biometry and BLE
- Decentralized biometric database where users have a full control over their biometry (GDPR compliant)
- Face recognition of people wearing masks

Contribution to standards

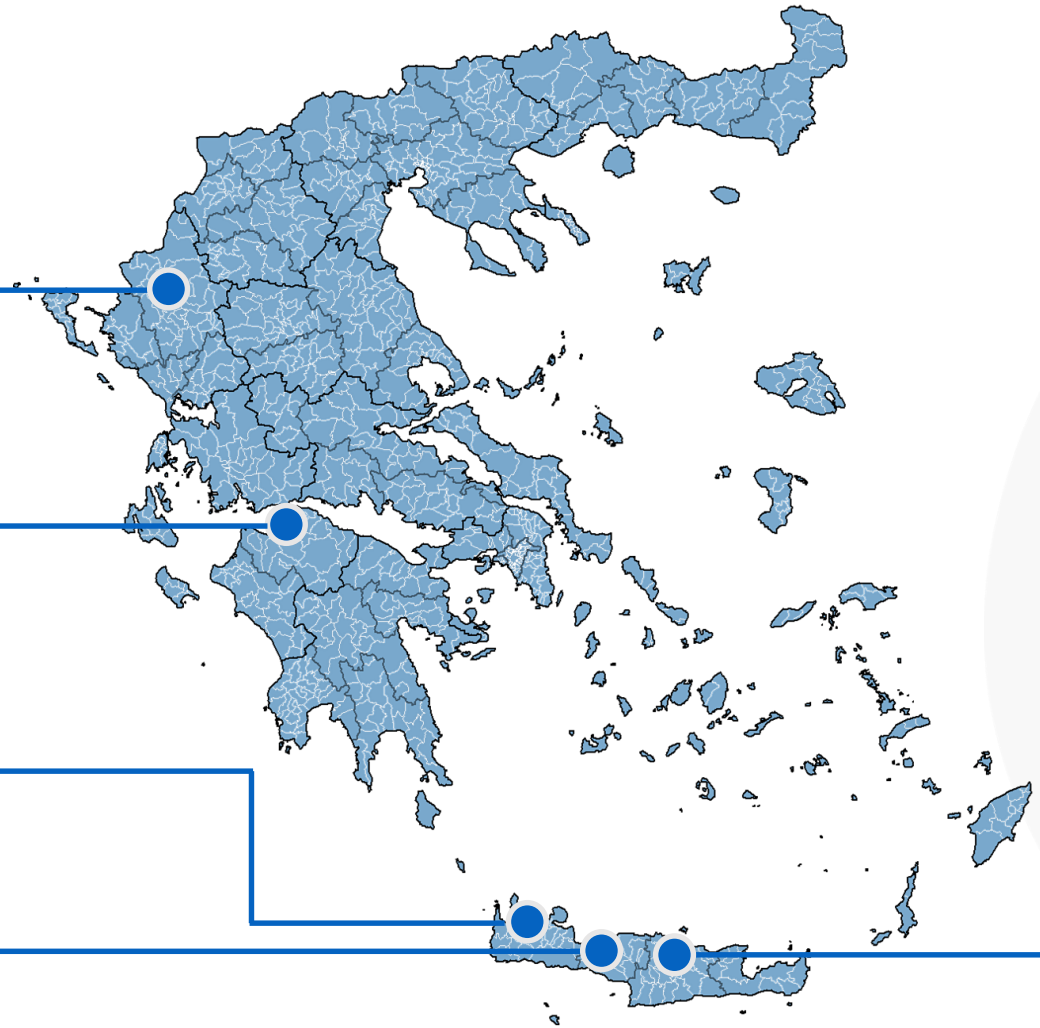
Emmanouil G. Spanakis, Ph.D.

FORTH

Panacea
People-centric cybersecurity in healthcare

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

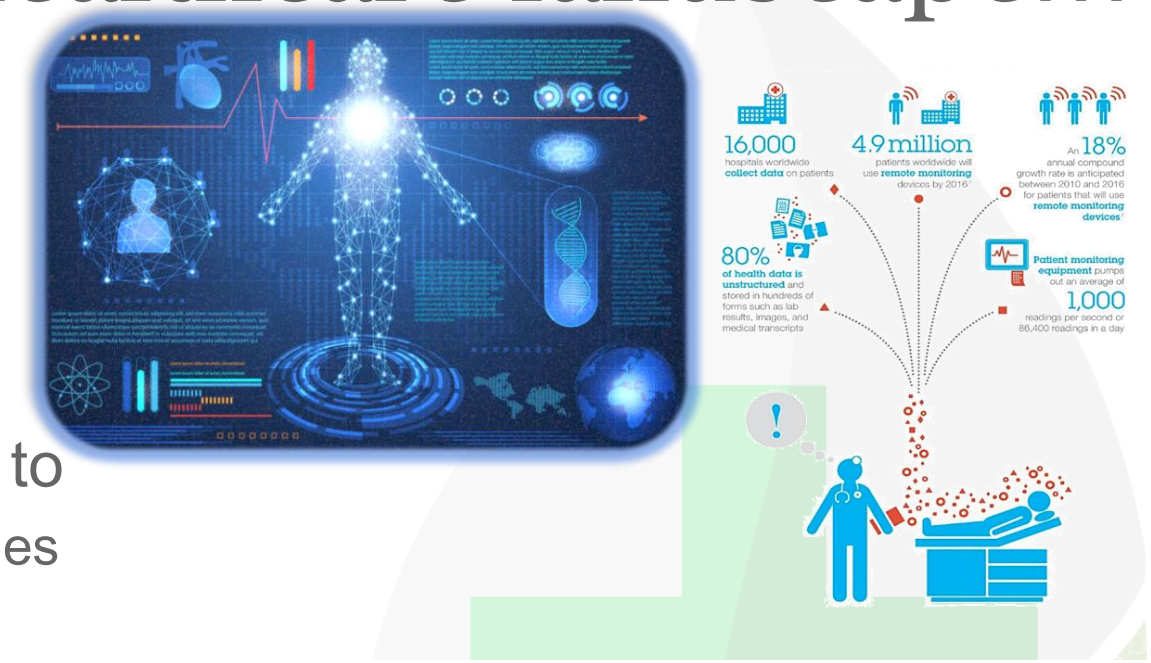
FORTH



- Department of Biomedical Research, **Ioannina**
- Institute of Chemical Engineering, **Patras**
- Institute of Petroleum Research **Chania**
- Institute for Mediterranean Studies, **Rethymno**
- Institute of Astrophysics, **Heraklion**
- Institute of Applied & Computational Mathematics, **Heraklion**
- Institute of Electronic Structure & Lasers, **Heraklion**
- Institute of Molecular Biology & Biotechnology, **Heraklion**
- Institute of Computer Science, **Heraklion**
- Crete University Press **Heraklion**

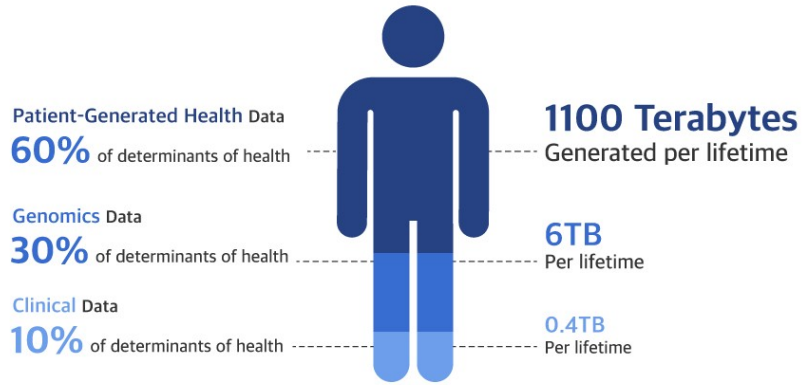
Panacea
People-centric cybersecurity in healthcare

The healthcare landscape…



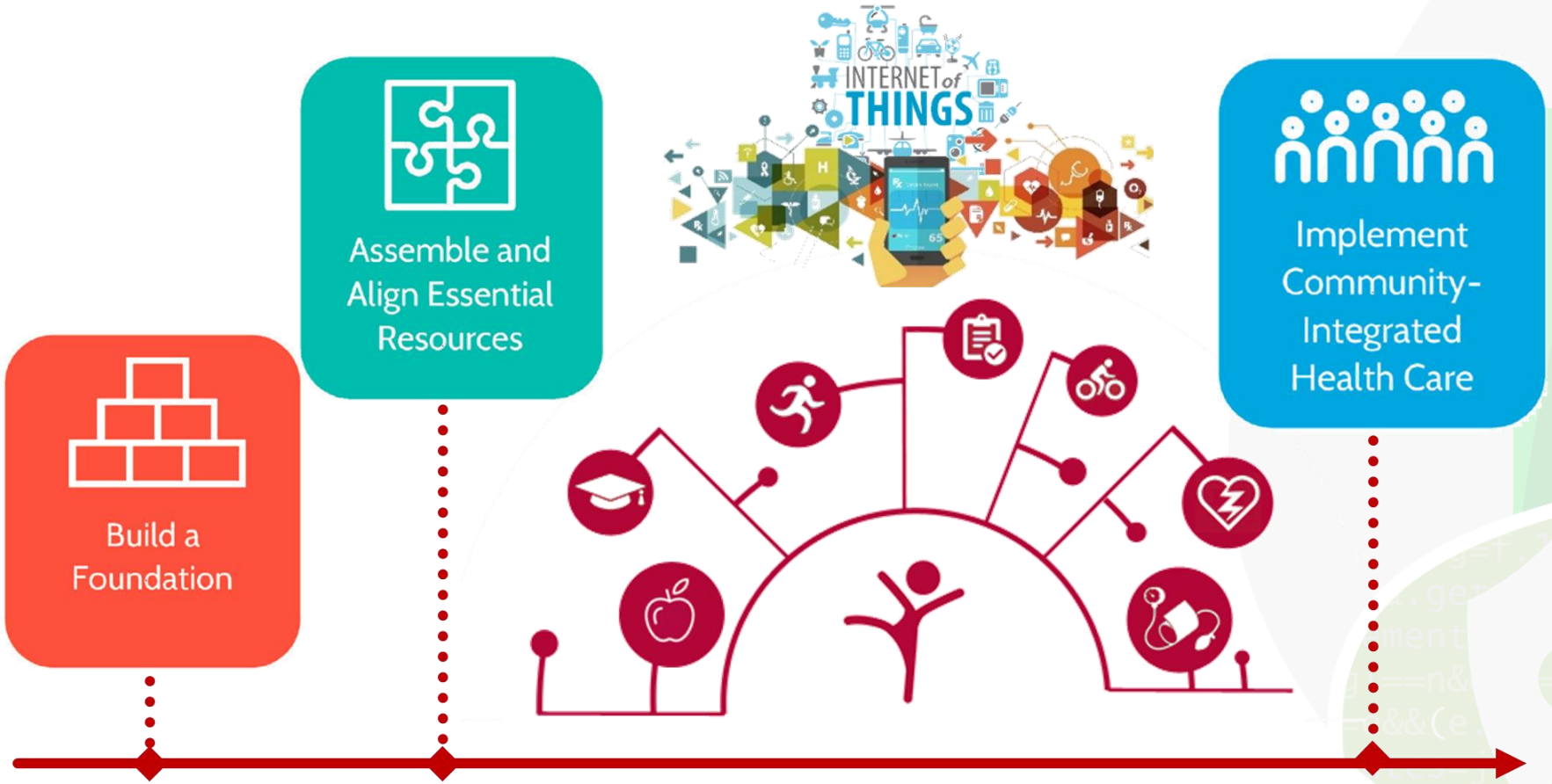
- Healthcare is a vast
  - applications in healthcare are endless
  - smart devices and Io(M)T have infiltrated into healthcare spaces
- The ambition is to create an *ecosystem* able to
  - empower patient/citizens in their daily care activities
  - improve how physicians deliver healthcare
  - change future strategies for healthcare organizations
  - affect diagnostics, treatments and patient health management
- The big caveat though in healthcare:
  - more connected devices/apps/ICT systems ➔
  - larger attack surface ➔
  - security is a significant challenge for healthcare organizations
    - *(where security is not suboptimal)*

"Exponential Growth and Important Role of PGHD"



Source: "The Relative Contribution of Multiple Determinants to Health Outcomes", Lauren McGover et al., Health Affairs. 33. no.2(2014)

Personal Health Systems to reassemble Healthcare



Background

- Idemia is part of ISO SC 37
  - Technical Report : ***TR 21419 "Information technology - Cross jurisdictional and societal aspects of implementation of biometric technologies - Use of biometrics for identity management in healthcare."*** was set on stand by
  - Reasons:
    - No Contributors
    - No editor
- Idemia proposed to contribute capitalizing the output of PANACEA EU project – with the aim of volunteering partners from PANACEA
  - FORTH supported this ACTION
    - expertise in developing novel ICT technologies in the wider context of predictive, personalized, preventive and participatory (the P4) medicine aiming at the research of personal e/m-health systems, devices and pervasive mobile monitoring

Contributions

- January 2020, an ISO committee member accepted to be the editor, and TR21419 was re-opened
  - https://www.iso.org/standard/80580.html
  - huge potential
- May 2020: TR is open for contribution: Forth + Idemia provided input
- July 2020: contribution was accepted
- Now: new draft is available, open for contribution…

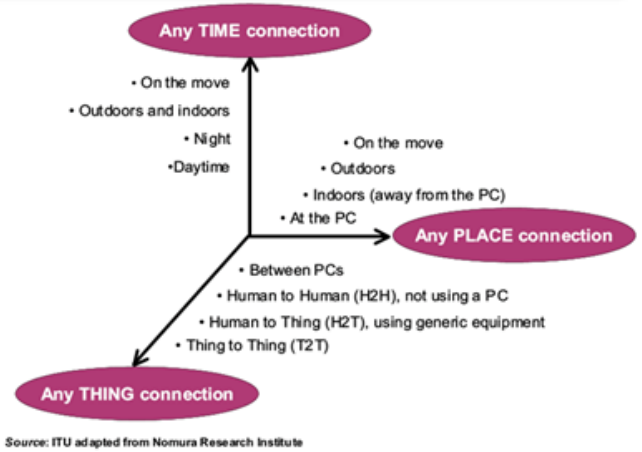
Starting point

- The “inactive” draft suggested the following areas where biometrics could bring value
  - “Universal” Identity management of healthcare related personnel
  - Access to medical records – must be shared AND protected
  - Safe home care / telecare emergency care
  - Easy checking of patient identity
  - Identity theft to access medical treatment
  - Ensure medical staff’s identity and qualification at the point of care
  - Correlation of medical files for research purpose
- It is on these domains that FORTH and IDEMIA provided input

Panacea
People-centric cybersecurity in healthcare

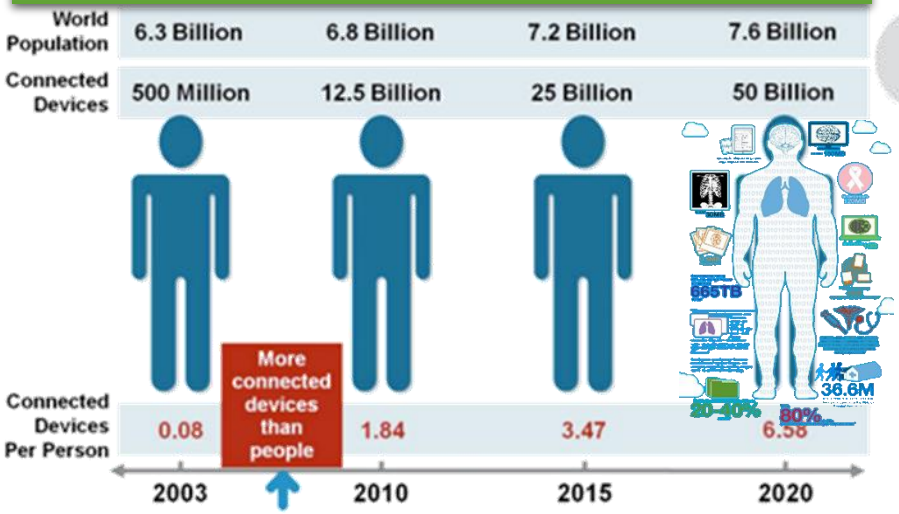
The landscape…we need to protect

Future Networks trends

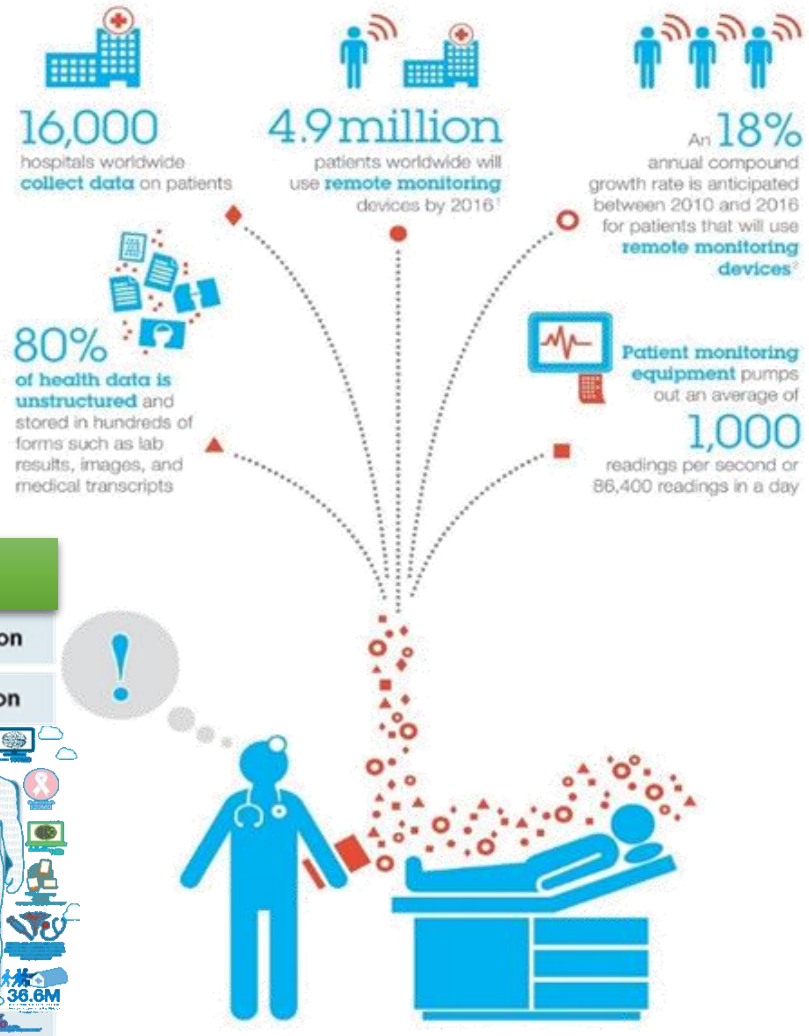


Source: ITU adapted from Nomura Research Institute

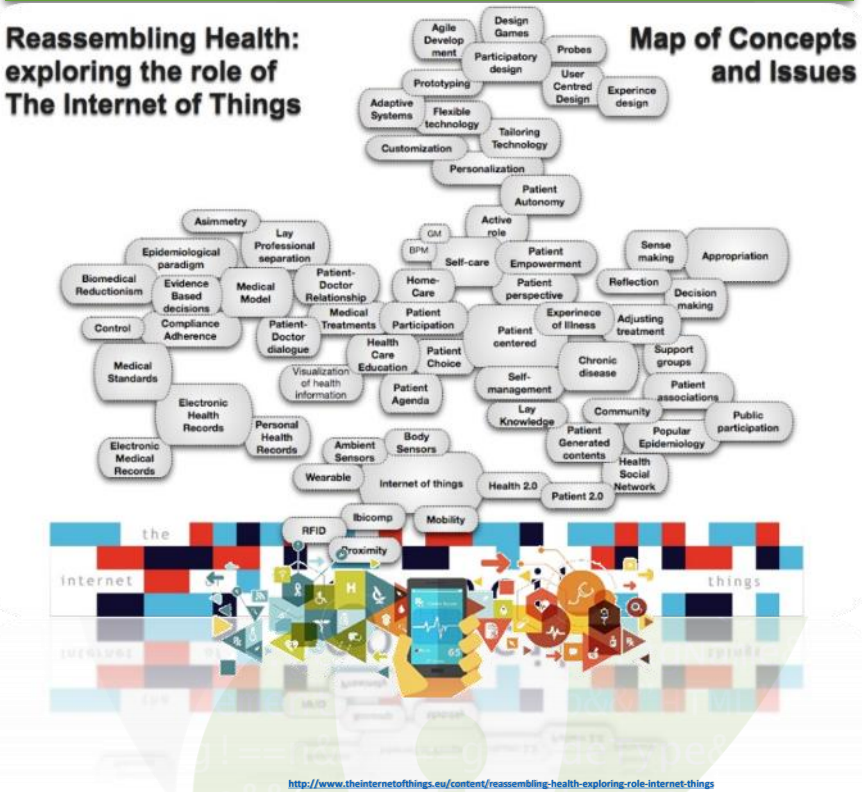
"Things" connected to the internet



Source: Cisco IBSG, April 2011



Future Personal Health Systems and trends

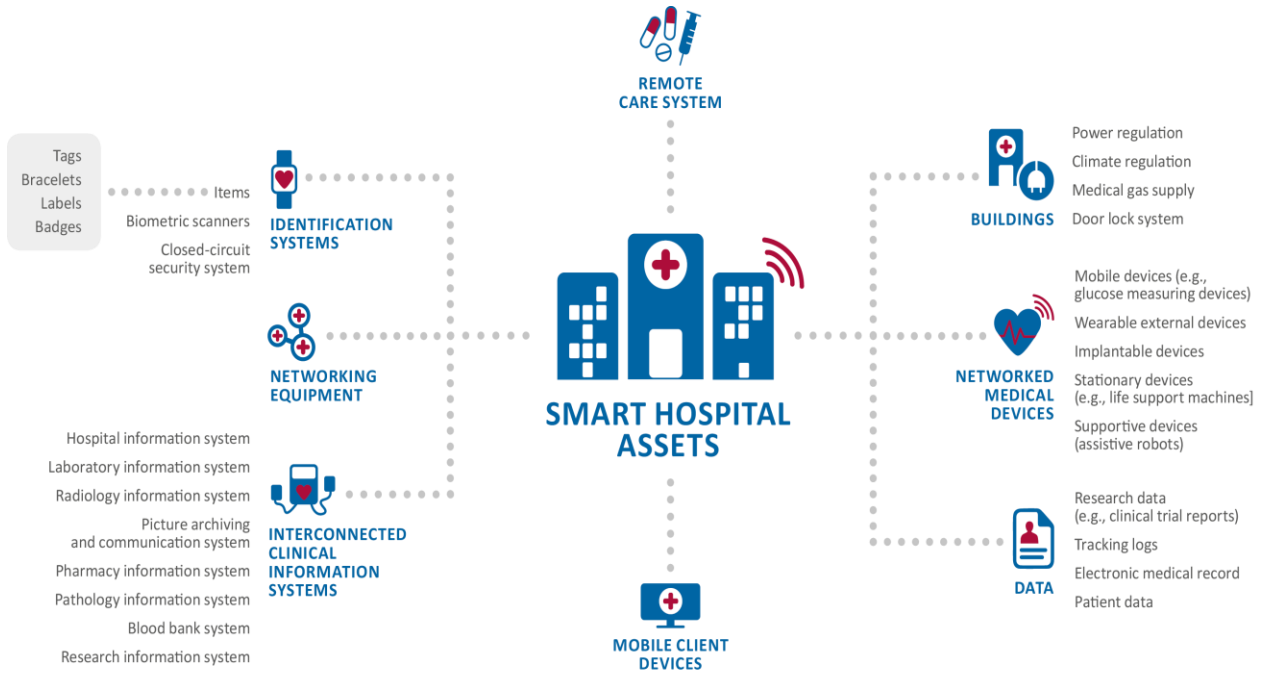


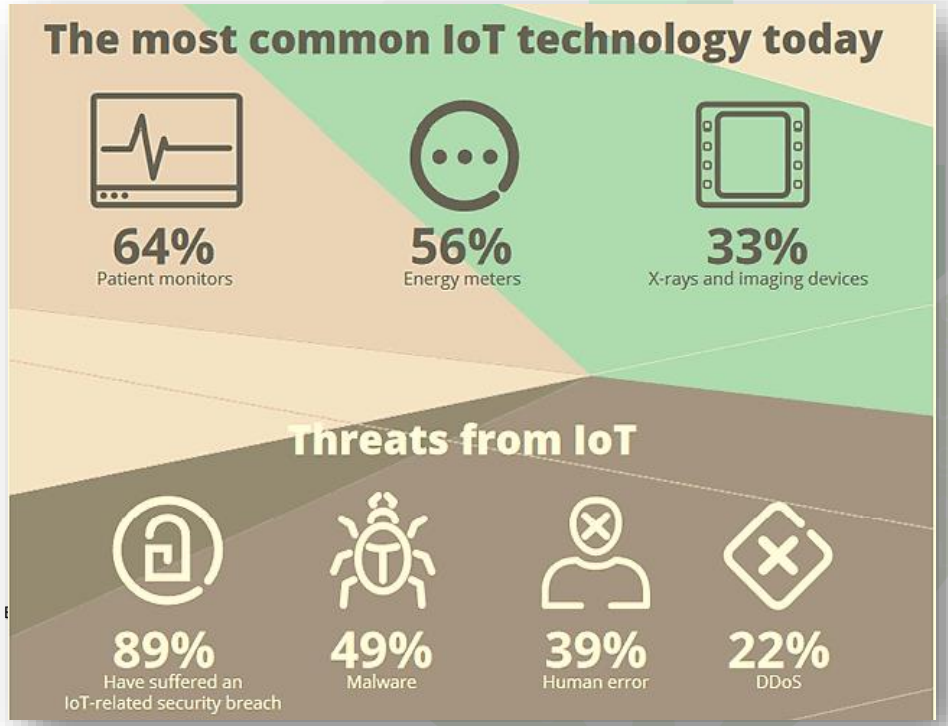
http://www.theinternetofthings.eu/content/reassembling-health-exploring-role-internet-things

Assets to be protected

Traditional vs. Smart (e)hospital – what assets to protect in terms of access

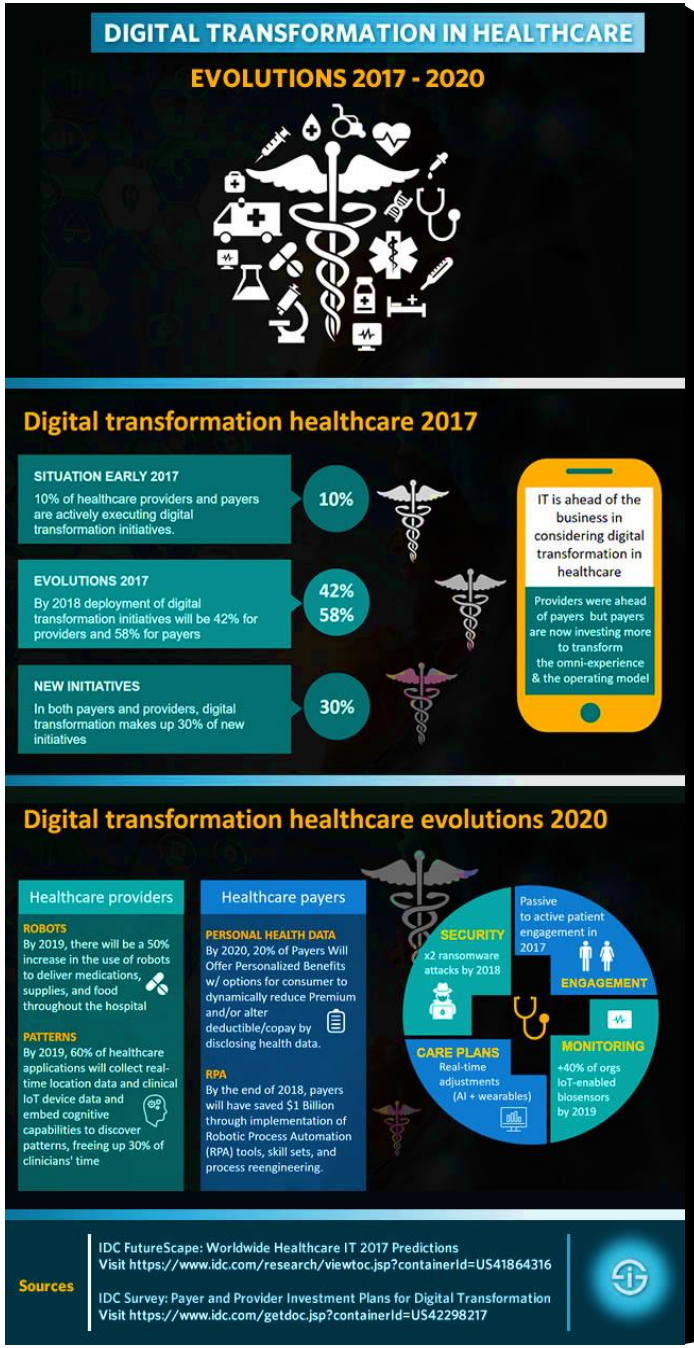
- A smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on IoMT.

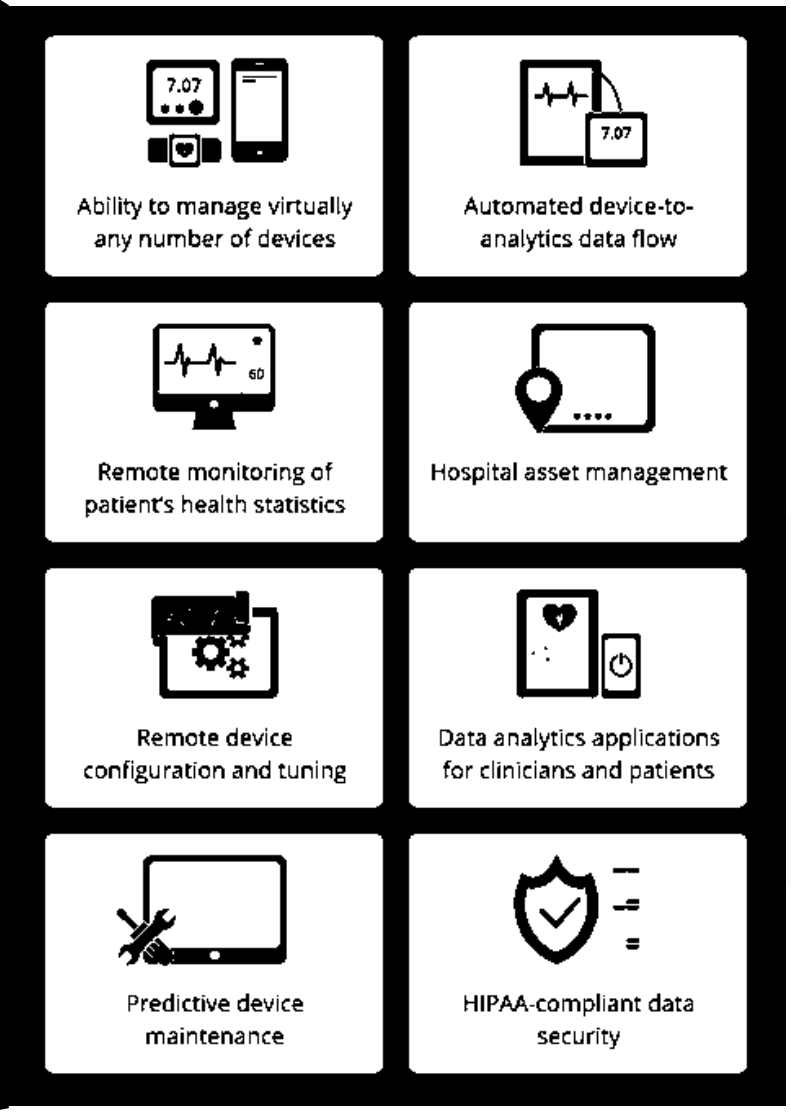




Source: ENISA, Cyber security and resilience for Smart Hospitals. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
State of IoT Healthcare infographic by Aruba Networks. https://www.i-scoop.eu/internet-of-things-guide/internet-things-healthcare/ - A. Lymberis, pHealth 10, Berlin, 26--28 May 2010

…benefits for healthcare





"More and more care will be delivered that needs to be safeguarded"

Technologies today can provide the technical component.

Only commitment at the highest levels can provide the policy component.

As long as humans behave like humans, you can never eliminate CyberRisks!

Panacea
People-centric cybersecurity in healthcare

Thanks you for your attention

- Questions…?