Digital Transformation and Information Security Challenges in Hospital Operations

Dražen Milković

Mr.sc.e.e., UHC Zagreb

Information systems in practice are very often developed with the presence of information solutions as isolated islands

- **Challenges:** lack of flexibility, adaptation capacity, improvements
- **Final goal:** integrated approach with the **patient oriented health services** and the patient safety

Is it different with the Information Security ?

„Islands"

Vs.

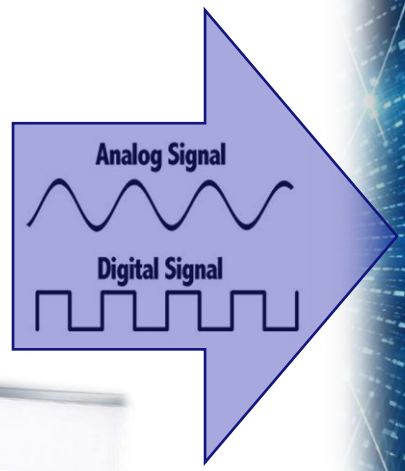
Everything is connected!

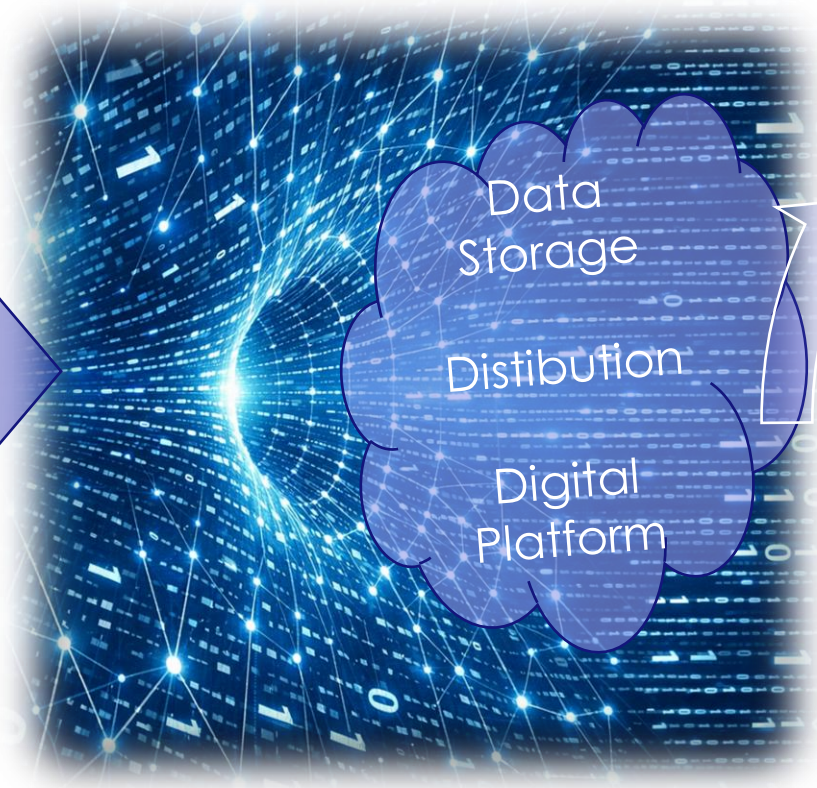
Are we cyber secure enough?

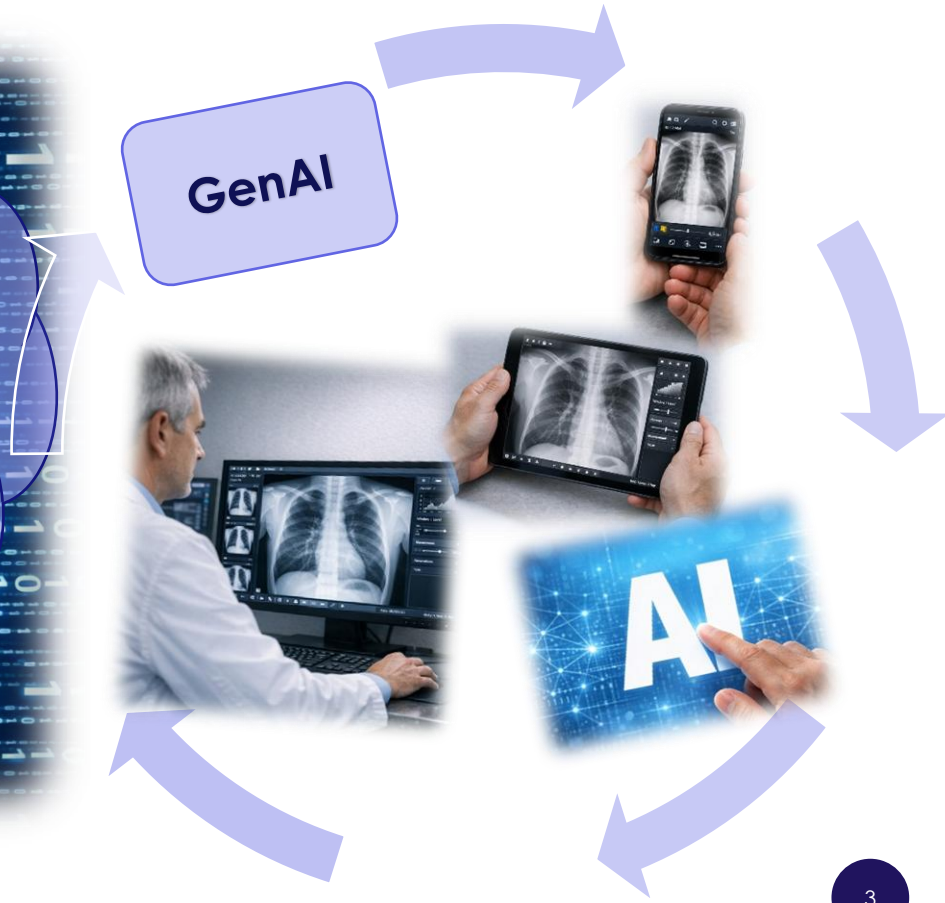
Digitalisation – as a **begining of** the **digital transforamtion**

- process of **converting analog** content **into** a **digital** form
- data **stored** on electronic media **for** further **processing**, **distribution**, and **retention**

Documents, images, audio, video, ect.

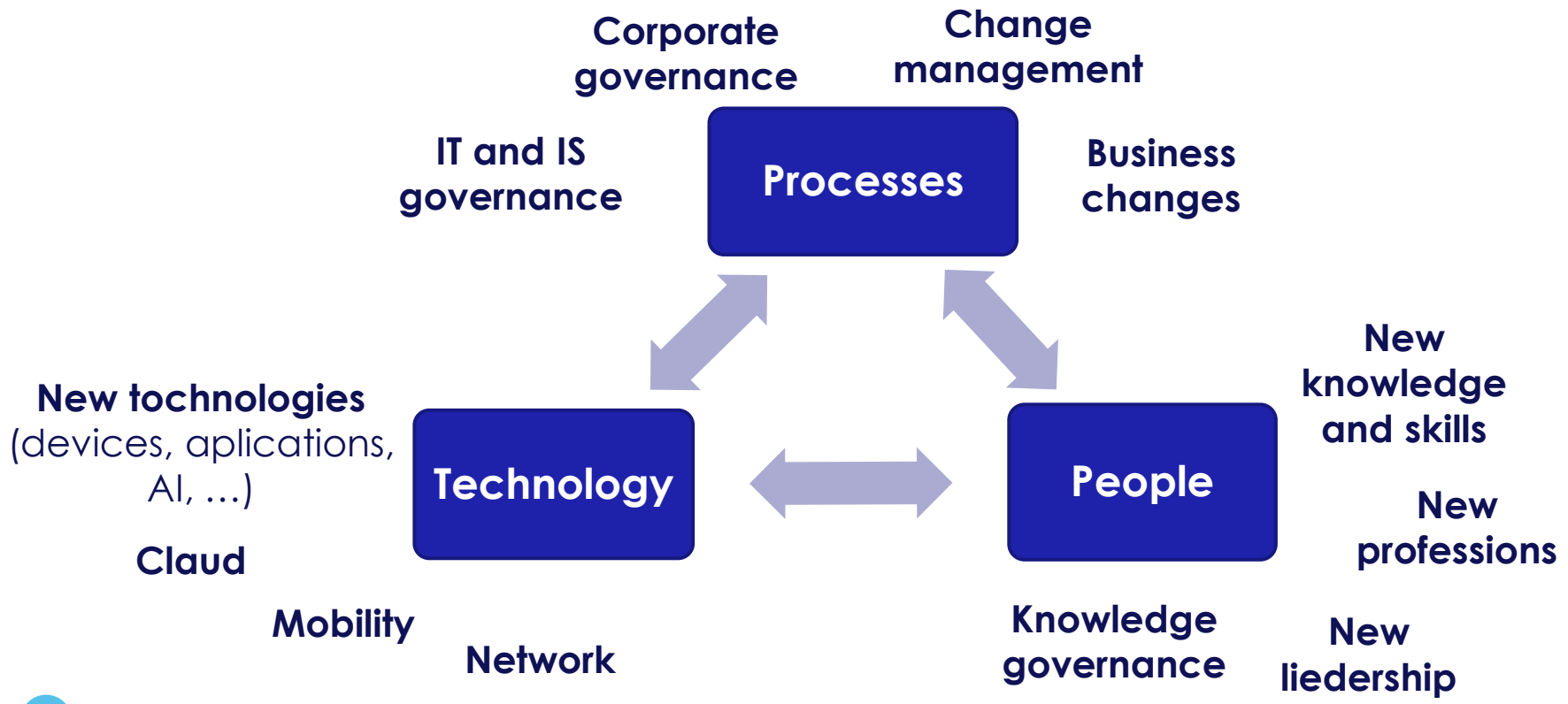






Digital transformation - as a **journey through constant changes** in business

- **Intensive utilisation of digital technologies**
- Today it is **no** longer a **matter of choice**, it has become **inevitable and necessary**



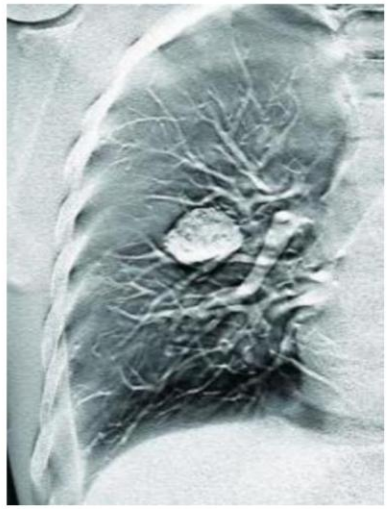
Digital transforamtion in Radiology - Big Data

- Digital diagnostic technology (devices) – Modalities
- X-ray, CT, MRI, Ultrasounds, ...
- Sources of imaging material in medicine

Analog

Standard X-ray Image

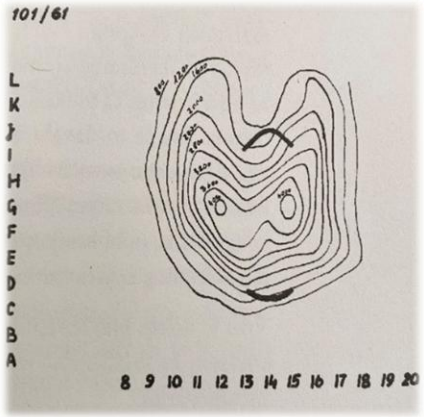
Digital



Digital 3D Image
CT (Computed Tomography)

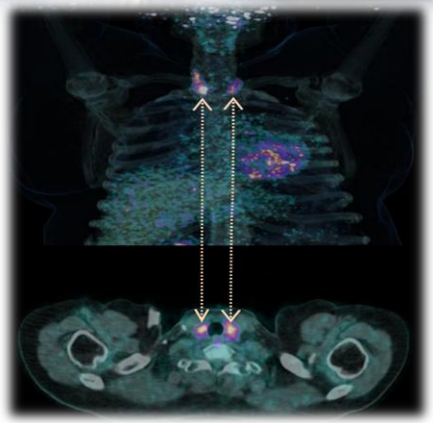
Digital transforamtion in Nuclear medicine

Scintillation detector for external measurements



Manual thyroid scintigraphy
(1962. UHC Zagreb)

PET/CT diagnostic imaging system
(Positron Emission Tomography / Computed Tomography)



3D fused PET/CT imaging of the thyroid gland
(2012. UHC Zagreb)

Radiopharmaceutical:
glucose analogue (FDG)
+ fluorine(18F)
positron-emitting isotope

Digital transforamtion in Radiotherapy

- **Radiotherapy in oncoclgy**
  - ionizing radiation for treatment of malignant tumors
- **Oncology Information System (OIS)**
  - specialized, integrated software platform and databese for treatment managent
- The concept of **“radiology islands” versus** a **centralized integrated system**
  - one OIS for multiple devices

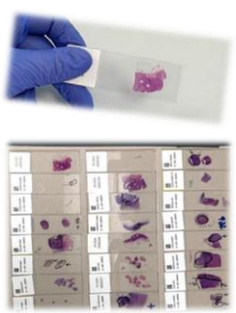
First Cobalt-60 beam machine, 1950-th *

Medical linear accelerator 70+ yars after

* https://en.wikipedia.org/wiki/Cobalt_therapy

Digital transformation of medical laboratory operations

Medical Proceses Automation

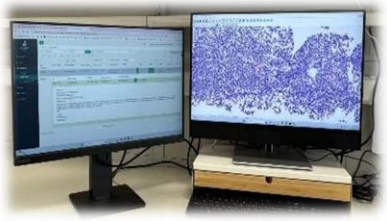


Microscop

Analog

Digital

Computer



Avanteges:

- **Eficiency -** results in minutes vs. hours
- **Quality -** minimizing dependence on human interaction
- **Standardisation -** proceses and technology
- **Integration -** interoperability between aplications, devices and health data records

Digital transformation across different hospital operations

Robot-Assisted Surgery
- UHC Zagreb, first robot 2019., Urology

Hospital Pharmacy auotmation
- CPC, isolators, robotized unit-dose medication preparation, …

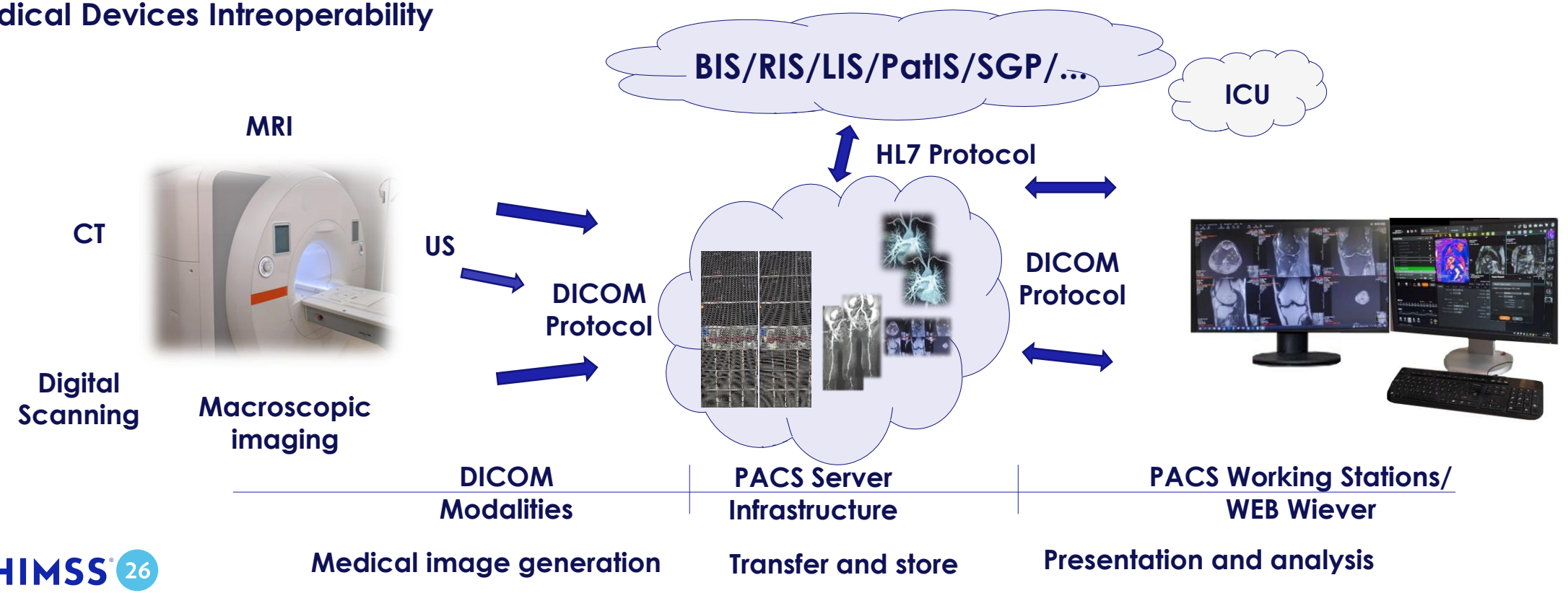
Speech to text
- Clinical Findings

Personalised medicine
- UHC Zagreb 2024.,
- New Clinical Depratment
- New laboratory (NGS)
- New HIS functionalities

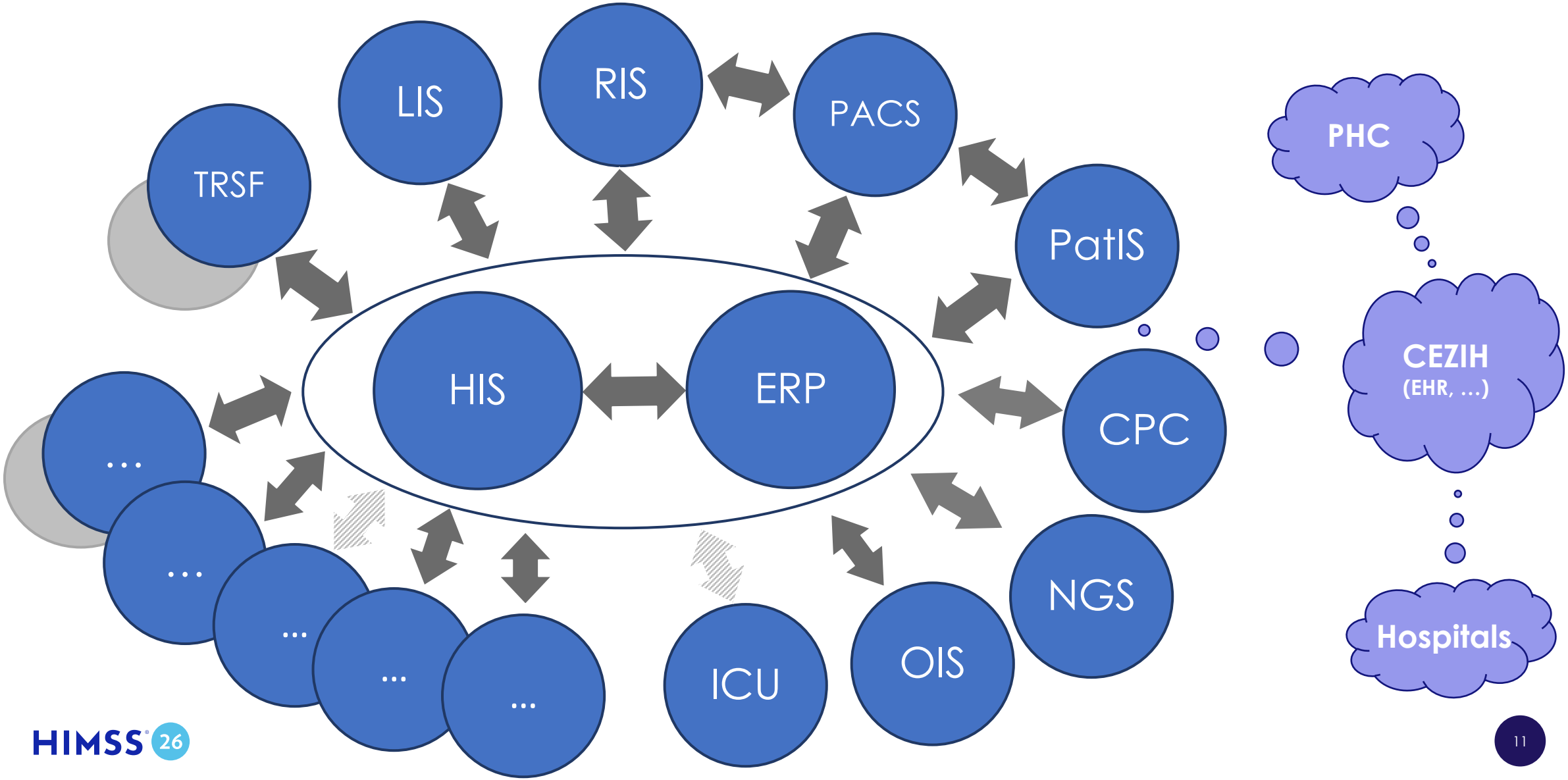
AI in practice
- Great potential expected
- New challenges in implementation and security

Standardisation, integration, interaction – open vs. closed standards

- **HL7 - FHIR** protocol (**H**ealth **L**evel Seven International - **F**ast **H**ealthcare **I**nteroperabillity **R**esources) – **Medical Data Inteoperabilitiy**
- **DICOM protocol** (**D**igital **I**maging and **C**ommunications in **M**edicine) – **Medical Images Intreoperabilty**
- **SDC protocol** (**S**ervice **O**riented **D**evice **C**onnectivity - IEEE 11073 SDC) – **Medical Devices Intreoperability**



UHC Zagreb - digital transfotrmation of the business operations

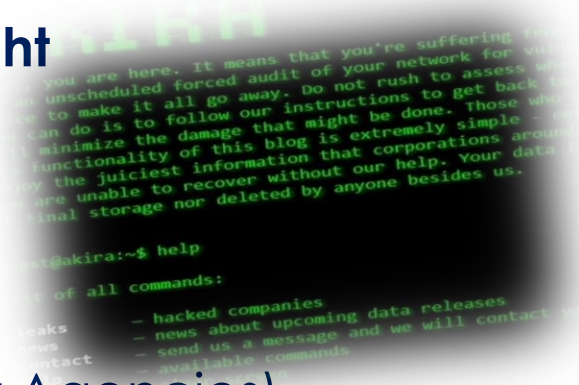


UHC Zagreb - Complexity of Business Environment ⬆

- **The largest National Hospital in Republic of Croatia**
  - Hosting **103 Reference Centers** of the Ministry of Health of the Republic of Croatia ⬆
  - **30 Clinics** and Clinical Departments ⬆
  - **Employees: 6.000+** ⬆
  - **Annual costs: 550+ mil. EUR (2023.)** ⬆
- **Complex ICT Infrastructure with a variety of Healthcare Systems, Digital Idintiies, Supply Chain, ect.** ⬆

Cybersecurity Incident – Not IF, but WHEN it happens

Incident occurrence: Thursday 27 June 2024 in the **first hour after midnight**



- **Emergency Department claimed functionality problems**
- **IT service desk - 24/7** (on site support, incident verification)
- **Incident escalation** (Management, Contracting Vendors, Government Agencies)
- **Containment of incident** (immediate isloation of network segment, devices, services)

By the morning hours, all teams had been notified, gathered and service recovery activities were initiated

Cybersecurity Incident – What to do when it happens?

Working teams continuously committed to the recovery:

- **Internal ICT team**
- **Vendors** for **critical ICT services and IS**
- **CSIRT** – Cybersecurity Incident Response Team (NCSC)
- **Ministry of the Interior** of the Republic of Croatia
- **Hospital Directorate** (crisis communications)
- **Internal Incident Response Team** (recovery coordination)
- **Vendors** for varieties **of Hospital Devices and Information Systems**

Cybersecurity Incident – Incident Recovery

- **Successive recovery of** individual **servers** and application **services** within the **new network segment**

- **Cyber Forensics**
  - Identification of the **attack vector**
  - Detection of **commonly used attacker tools**
  - Detection of **encrypted servers, application services, databases**
  - **Acquisition of digital forensic artefacts** for further analysis

Cybersecurity Incident – Incident Recovery

- **Hospital Information System -** available and **operational** next day after incident
- **All clinics continuing to deliver health services**, some segments **with less capacity**
- **All Vendors cooperate in recovery processes**

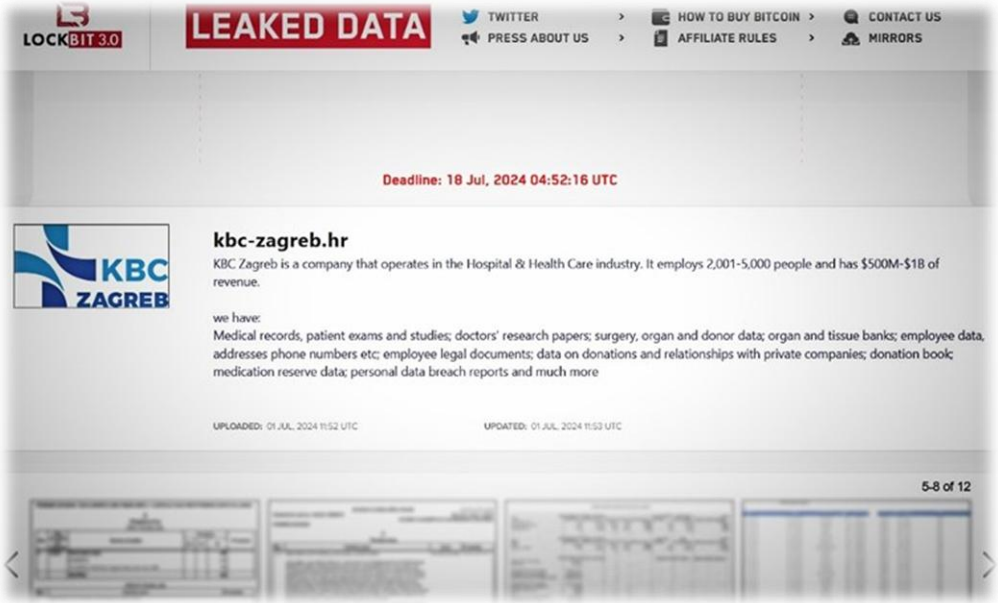
- **Back to the history of a paper work!**
  - **Patients have been** diagnostically **processed at the clinics**
  - **Doctors wrote the findings by hand**

*

* https://dnevnik.hr/vijesti/hrvatska/strucnjak-za-sigurnost-za-novu-tv-je-komentirao-kiberneticki-napad-na-kbc-zagreb---856332.html

Cybersecurity Incident – Incident Recovery

- **Announcement about the cyber attack -** 4th day after the incident
  - Platform: X
  - Profile: HackManac
  - Cybercriminal organization: **LockBit3.0**
- **Ransomware attack –** A ransom is regularly demanded for data recovery
- **Deadline**: 18 July 2024



- **Croatian Government - No negotiation** with cyber attackers
- **All resources dedicated to the recovery** of hospital services

Key Takeaways ?

- **UHC Zagreb** had **not been permanently disabled** in **providing patients care**
- **Patients care** was **carried out continuously but** at the beginning **with somewhat delay**

- **Initial attacker access** was achieved through the execution of the **„identity theft"** threat
- **Proactive approach,** monitoring, early **threat detection** and **prevention** (SIEM/SOC, etc.)
- **Multi-layered cybersecurity (Defense in Depth)**
- **Strenhgtenig sybersecurity** resilience by **optimal egagemnaet** of **internal and external resources** (supply chain management)
- **Committed and reliable Vendors** (SLA, NDA, DPIA, built-in cybersecurity, right to audit, etc.)
- **A systematic approach to protecting national cyberspace**

- **We will never be 100% cyber safe,** but we should be able to **reasonably protect** our **employees**, **patients** and our **business from cyber threats**

A systematic approach to protecting national cyberspace

- **Croatia is among the first EU member states to transpose the NIS2 Directive into its national legislation:**
  - **Cybersecurity Act** (February 2024)
  - **Regulation on Cybersecurity** (November 2024)

- **The application of the law and** imlemetation of the **measures**, among other things, **basilally include:**
  - **categorization** of obligated entities
  - mandatory **incident reporting**
  - **risk management** (13 measures and 109 sub-measures)
  - **supply chain security**

- Primarily **aiming at strengthening** cyber resilience, **not punishment**
- **Compliance** should be **just the result of implemented** cybersecurity management **measures**

Challenges of the Information Security

Information security concerns of everyone in the organisation

(it is not someone else problem)

Information security must be integrated in Corporate governance and Culture of an organisation

Investing in Information security is not a Cost, it is an Investment

A hope is not the Strategy

HIMSS 26
EUROPE

Thank you