Digital Health

Spring 2025

UNIVERSIDAD POLITÉCNICA DE MADRID

Agenda

# 10 Challenges in Digital Health: Cybersecurity, Interoperability (Interconnectivity) Confidentiality, privacy, ethics, governance

- Questions from Last Week
- Learning Objectives: Discipline literacy, critical analysis skills, applied and integrative learning, oral communications.
- Icebreaker: Who is your favorite musician?
- Definitions, discussion, lecture

IT Challenges In The Healthcare Sector

01 Cybersecurity Threats

02 Interoperability Issues

03 Legacy Systems

04 Data Privacy Concerns

05 Integration Complexity

06 Limited Budgets

07 Resistance To Change

08 Regulatory Compliance

Cybersecurity

Cybersecurity

Healthcare is vulnerable to cybersecurity risks and the stakes for patients are high.

According to IBM Security, each hospital data breach costs almost $11 million.

Stolen data in health records sells for more on the dark web than stolen credit cards.

Should a hospital pay a ransom?

- 2018, Hancock Regional Hospital (Indiana, USA) was encrypted with SamSam malware and needed to pay ransom in bitcoin. They paid **$55,000** in bitcoin
- February 2024, A ransomware gang, called Lockbit hacker group, said a Chicago safety-net hospital had two days to pay nearly **$900,000** ransom or else it will leak patients' data

- https://www.beckershospitalreview.com/cybersecurity/ransomware-gang-gives-hospital-2-days-to-pay-900k.html
- https://www.beckershospitalreview.com/cybersecurity/we-did-what-a-hospital-does-every-day-how-hancock-regional-responded-to-a-ransomware-attack.html

Cybersecurity

CYVATAR.AI
THE CHANGE HEALTHCARE RANSOMWARE ATTACK:
A Comprehensive Analysis and Lessons for the Healthcare Sector

- Change Healthcare, a unit of UnitedHealth Group, handles more that 15 billion transactions annually and 1/3 are health care claims.
- March 2024, Change Healthcare Systems had a ransomware attack carried out by ALPHV/Blackcat hacking gang, stole 6TB data
- Effected 190 million Americans
- The company paid **$22 million** in cryptocurrency.
- Physician practices across the U.S. were disrupted for months operationally and financially.
- Health care cybersecurity focuses on privacy protection, not attacks

Cybersecurity

- Hospitals and clinics are attractive targets for cyber criminals because
  - Size
  - Dependence on technology
  - Sensitive data
  - Vulnerable to disruptions.
- Healthcare trails other industries because their defenses are less secure and they have trouble attracting top cybersecurity talent because other industries pay better.

- https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

Cybersecurity

- Global problem….Data breaches and cyber attacks

iZOOlogic
A ransomware attack disrupted the
operations of a French hospital

- Data was stolen in Simone Veil Hospital, Cannes, **France** cyber attack in 2024. The ransomware group LockBit claimed the attack .
  - The hospital **did not pay** and 61 GB of data were released on the dark web.
  - 1/3 surgeries were cancelled and medical staff needed to use pencil and paper patient charts.

- A supply chain attack affected 100 **Romania**n hospitals via their healthcare management system, Hipocrate Information System
  - Backmydata ransomware, which encrypted data pertaining to hospitals across the country, asking for $175,000 in bitcoin.

More cyberattacks in Europe

2023

- University Medical Center, **Maastricht** (MUMC+) and the cybersecurity agency Z-CERT being hit by the pro-Russian hacker group Killnet which launched a Distributed Denial-of-service (DDoS) attack.

- Websites of nine hospitals in **Denmark** were shut down due to DDoS attacks performed by a relatively new hacker group known as Anonymous Sudan.

More cyberattacks in Europe

- Hospital Clínic de **Barcelona** experienced a ransomware attack which forced thousands of appointments, hundreds of non-urgent operations and patient checkups canceled, including radiotherapy visits, because staff were not able to access patients’ clinical records.

- University hospital in **Brussels** hit the Centre Hospitalier Universitaire Saint-Pierre where staff were forced to use paper records, and ambulances and medical vehicles had to be diverted to neighbouring establishments out of precaution.

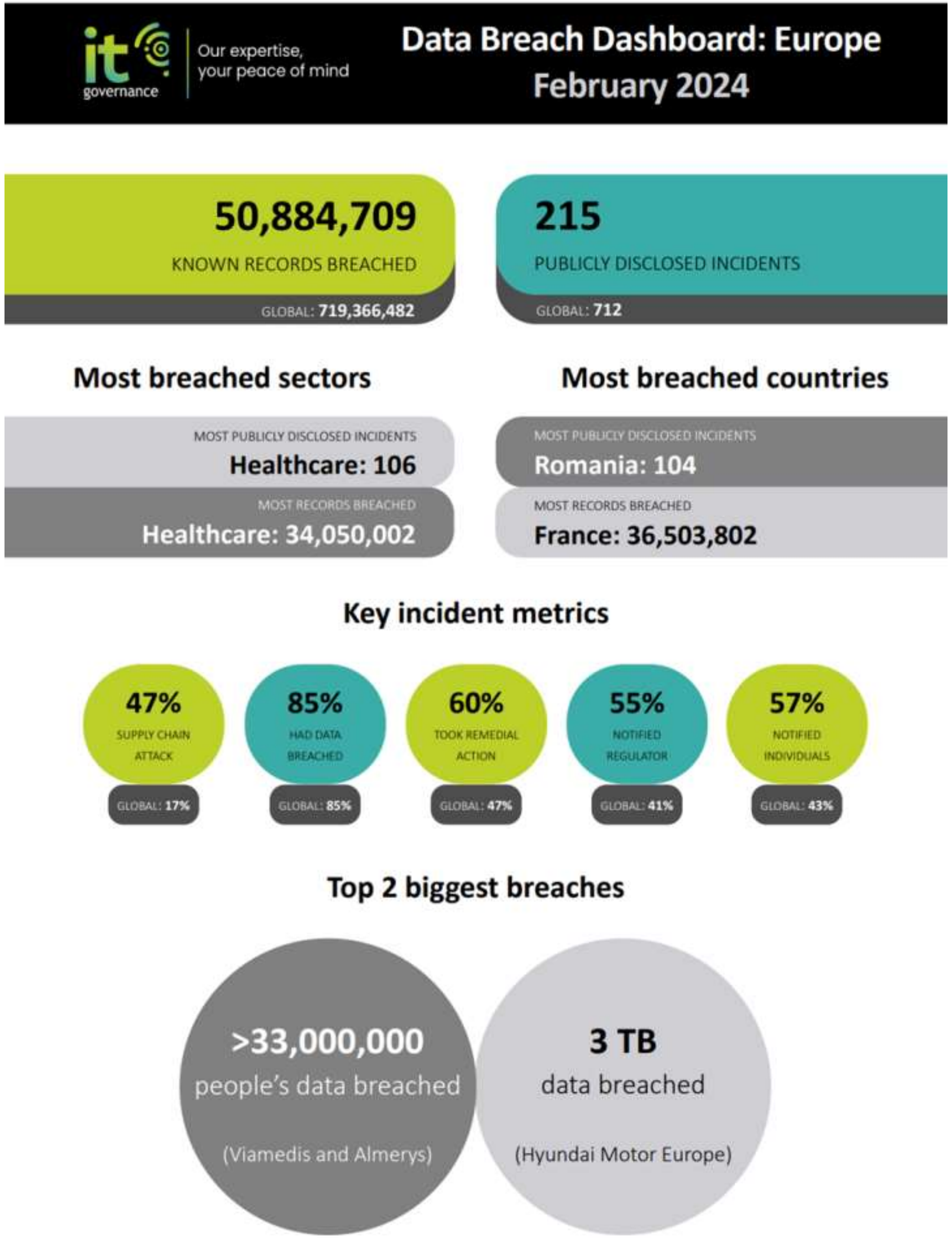
EU Health Cybersecurity

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

- The European health sector experiences a significant number of incidents
  - Most of the incidents are in hospitals but also health authorities and the pharmaceutical industry
  - Ransomware is the primary threat because most health organizations do not have a dedicated ransomware defense program.
  - Electronic medical records are most frequently targeted with more than half of incidents aimed at stealing patient data.

How often do threats happen?

- In the U.S., 92% of Healthcare Organizations experienced a Cyberattack in 2024
- Average number of attacks was 40, many detected before a major problem
  - https://www.hipaajournal.com



it governance | Our expertise, your peace of mind

Data Breach Dashboard: Europe February 2024

50,884,709
KNOWN RECORDS BREACHED
GLOBAL: **719,366,482**

215
PUBLICLY DISCLOSED INCIDENTS
GLOBAL: **712**

Most breached sectors

MOST PUBLICLY DISCLOSED INCIDENTS
Healthcare: 106

MOST RECORDS BREACHED
Healthcare: 34,050,002

Most breached countries

MOST PUBLICLY DISCLOSED INCIDENTS
Romania: 104

MOST RECORDS BREACHED
France: 36,503,802

Key incident metrics

47% SUPPLY CHAIN ATTACK — GLOBAL: **17%**

85% HAD DATA BREACHED — GLOBAL: **85%**

60% TOOK REMEDIAL ACTION — GLOBAL: **47%**

55% NOTIFIED REGULATOR — GLOBAL: **41%**

57% NOTIFIED INDIVIDUALS — GLOBAL: **43%**

Top 2 biggest breaches

>33,000,000
people’s data breached
(Viamedis and Almerys)

3 TB
data breached
(Hyundai Motor Europe)

https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-europe-in-february-2024-50884709-records-breached

Can the heart be hacked? Does someone want you dead?

Dick Cheney’s Fear of Heart….

Dick Cheney's Fear of Heart Device Hacks Justified, Experts Say - ABC News

- Dick Cheney's Fear of Heart Device Hacks Justified, Experts Say - ABC News

Can the heart be hacked? Does someone want you dead?

- In 2019, the U.S. Department of Homeland Security warned that 20 Medtronic products were vulnerable to short-range hacking.
- Hackable products include 16 implantable heart defibrillators -- an attacker could alter the settings of someone's device by manipulating its radio link.
- In-home bedside monitors for the defibrillators and programming computers used by doctors.
- The vulnerability may impact up to 750,000 devices.
- https://www.cnet.com/news/dhs-reveals-some-medtronic-heart-defibrillators-are-vulnerable-to-hacking/

Why are medical devices so vulnerable?

- More targets when hospital devices are connected and not designed to be network managed

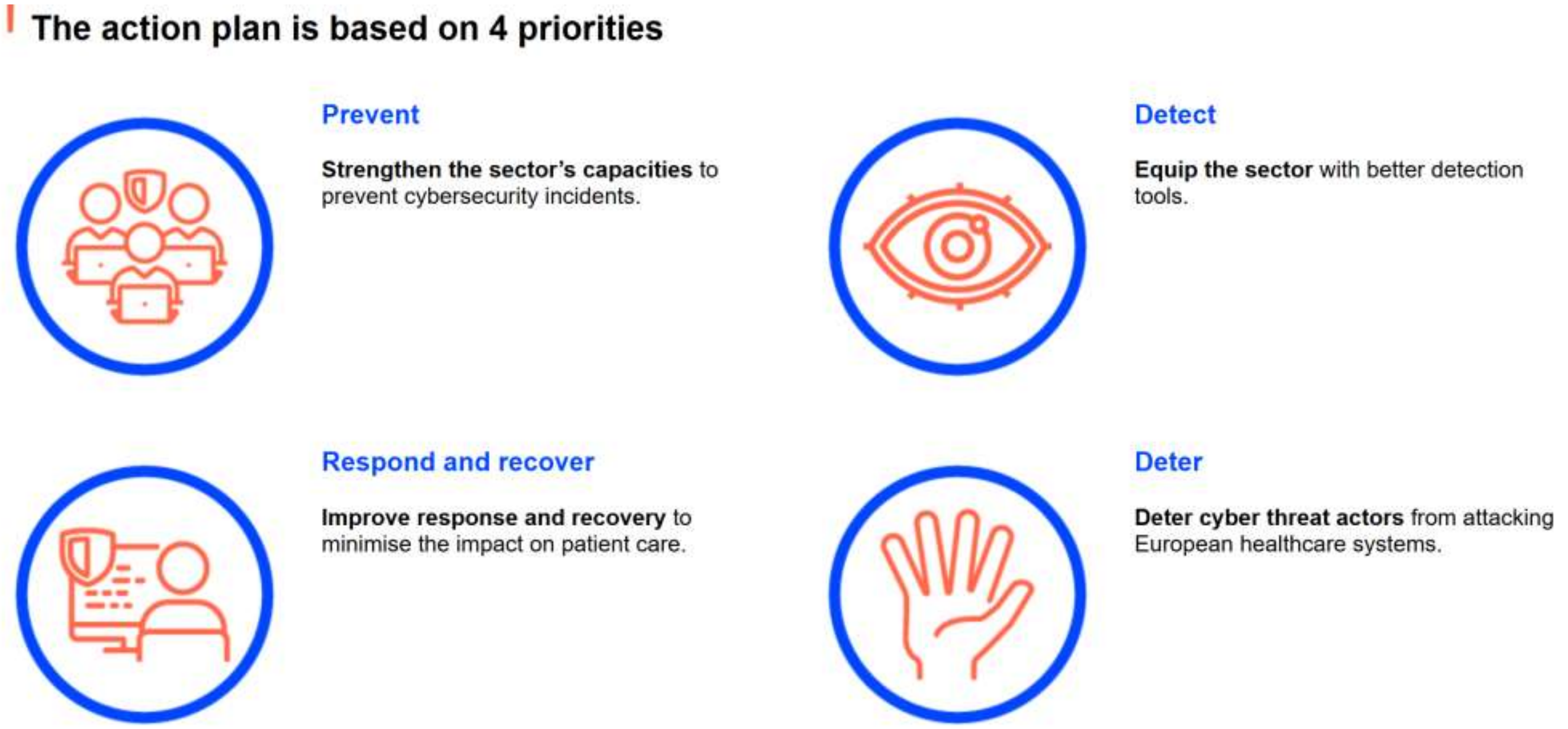
- Hospital IT staff need to understand dozens of different devices

- Patching and updating is complex

Why are medical devices so vulnerable?

- Manufacturers do not publish software/firmware eliminating scrutiny
- Risk assessment not comprehensive
- Personal data can be a matter of life or death
- Firewalls not robust
- Investment in latest tools does not always happen – many legacy systems

EU Action Plan



The action plan is based on 4 priorities

Prevent

Strengthen the sector’s capacities to prevent cybersecurity incidents.

Detect

Equip the sector with better detection tools.

Respond and recover

Improve response and recovery to minimise the impact on patient care.

Deter

Deter cyber threat actors from attacking European healthcare systems.

Cybersecurity Methods

Should hospitals practice fake cybersecurity attacks?

- Multiple layers using one-time passwords, biometric screenings, knowledge-based authentication, multiple access points
- Encryption, non-repudiation, firewalls
- Heuristic-based intrusion methods
- Antivirus tools
- Risk management, remediation, threat detection, vigilance and monitoring
- Experienced security team
- Incident response planning

What can a patient do to be protected?

- More scary articles
  - Hackers have the ability to access 3-D medical scans and add or remove images of malignant tumors, placing patients at risk of misdiagnosis (BenGurion University, Israel)
    - https://www.timesofisrael.com/israeli-researchers-show-medical-scans-vulnerable-to-fake-tumors/
  - Covid-19 research testing site attacked in Czech Republic
    - https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak

What can a patient do to be protected?

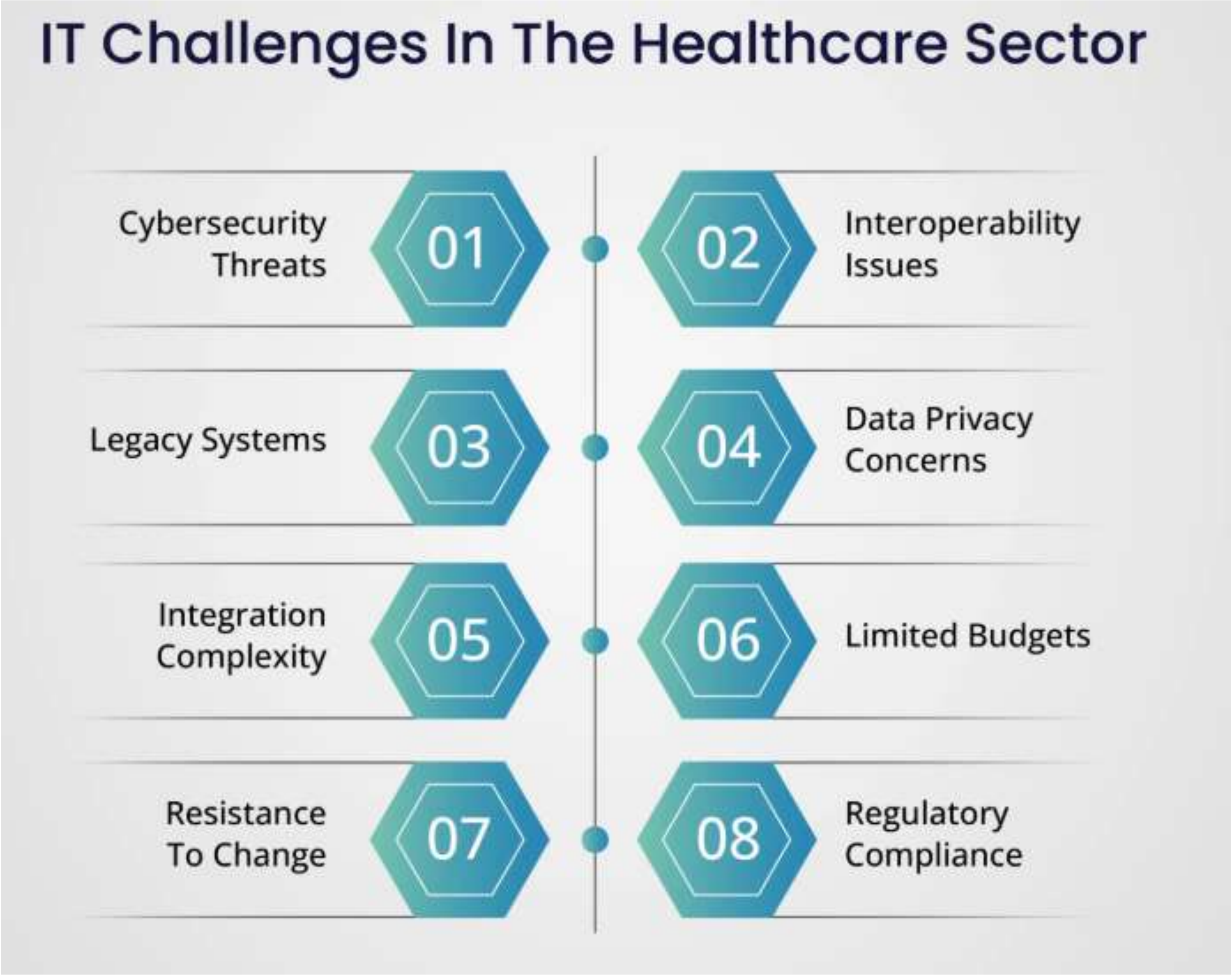
- Update passwords regularly
- Use strong unique passwords for different accounts
- Enable two-factor authentication on sensitive accounts
- Log out of accounts

Should a hospital explain the cybersecurity risks to patients?

Cybersecurity vendors: Cylera – “Safeguarding what matters most”

- “We are a patient-centric healthcare cybersecurity and intelligence company, changing how healthcare organizations protect and manage their medical and HIoT devices.” www.cyclera.com

New York City based company with employees in Europe, eg, Madrid



IT Challenges In The Healthcare Sector

01 Cybersecurity Threats

02 Interoperability Issues

03 Legacy Systems

04 Data Privacy Concerns

05 Integration Complexity

06 Limited Budgets

07 Resistance To Change

08 Regulatory Compliance

Interoperability

Interoperability Definition

- The ability of two or more different health information systems, applications, data sets or devices to connect, exchange, interpret, and use data cooperatively.
- Need standards for health data exchange architectures, application interfaces, message formats and vocabularies to enable data to be accessed and shared appropriately
- EMRs must be available and discoverable to use the patient information and clinical workflow in a meaningful way
- Bing Videos – Solution of one company, founded in 2022, HIPAA compliant, no coding

HL7® FHIR®

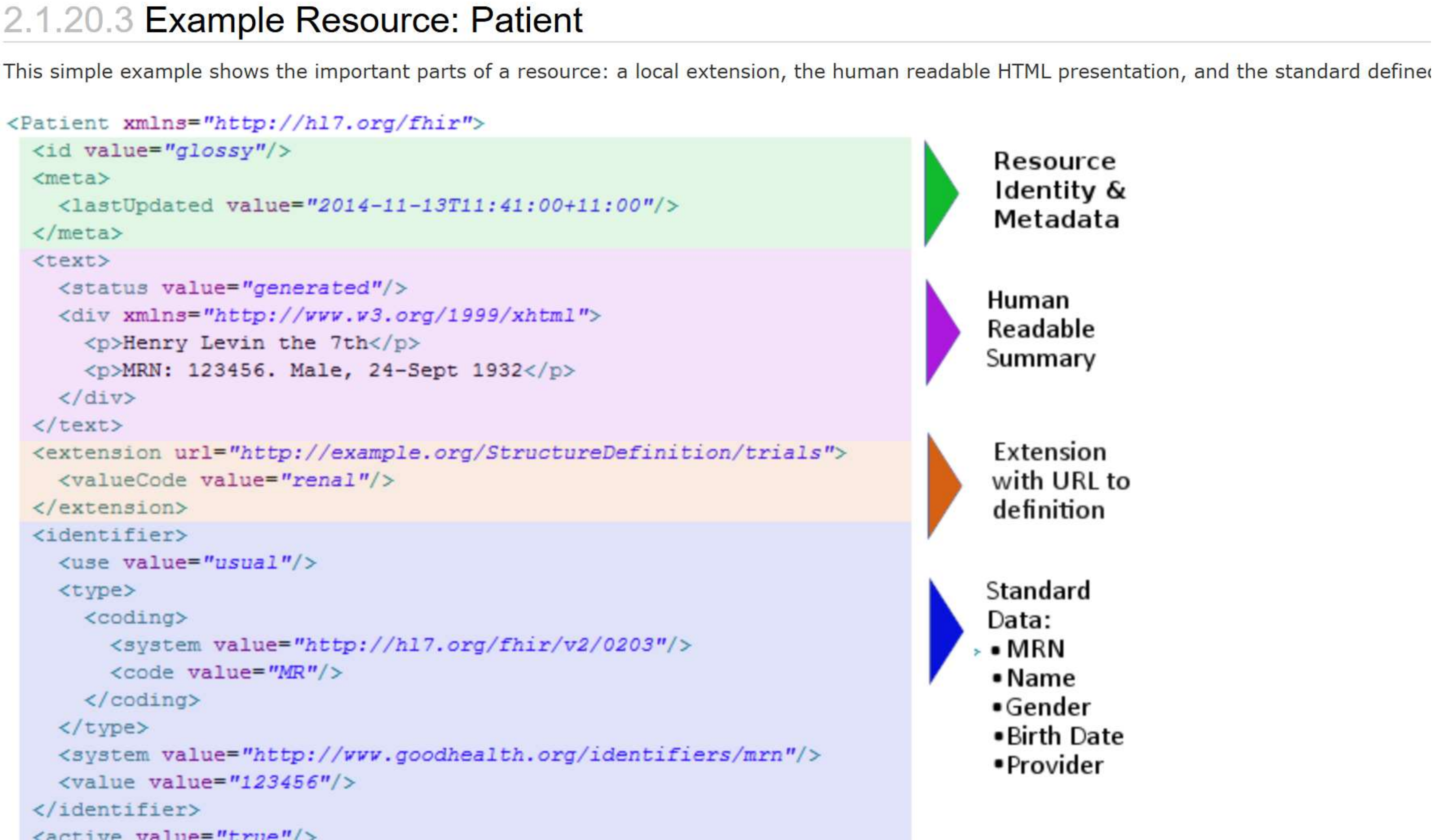
(Fast Healthcare Interoperability Resources)

Interoperability Solutions

- Founded in 1987, Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization
- Provides a framework and standards for the exchange, integration, sharing and retrieval of electronic health information
- Supports clinical practice and the management, delivery and evaluation of health services.

Interoperability Solutions

- HL7 FHIR is a standard for exchanging healthcare information electronically.
- Check out the complexity…
- http://hl7.org/fhir/index.html
- http://hl7.org/fhir/summary.html



2.1.20.3 Example Resource: Patient

This simple example shows the important parts of a resource: a local extension, the human readable HTML presentation, and the standard define

```
<Patient xmlns="http://hl7.org/fhir">
  <id value="glossy"/>
  <meta>
    <lastUpdated value="2014-11-13T11:41:00+11:00"/>
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">
      <p>Henry Levin the 7th</p>
      <p>MRN: 123456. Male, 24-Sept 1932</p>
    </div>
  </text>
  <extension url="http://example.org/StructureDefinition/trials">
    <valueCode value="renal"/>
  </extension>
  <identifier>
    <use value="usual"/>
    <type>
      <coding>
        <system value="http://hl7.org/fhir/v2/0203"/>
        <code value="MR"/>
      </coding>
    </type>
    <system value="http://www.goodhealth.org/identifiers/mrn"/>
    <value value="123456"/>
  </identifier>
  <active value="true"/>
```

Resource Identity & Metadata

Human Readable Summary

Extension with URL to definition

Standard Data:
- MRN
- Name
- Gender
- Birth Date
- Provider

Interoperability Standards

- To share data, it must be structured and standardized
- To share data, the syntax of the exchange must be consistent
- Use a standardized vocabulary and codification, recognized widely
- Organizationally, there must be agreed upon policies, end-user processes, and workflows.

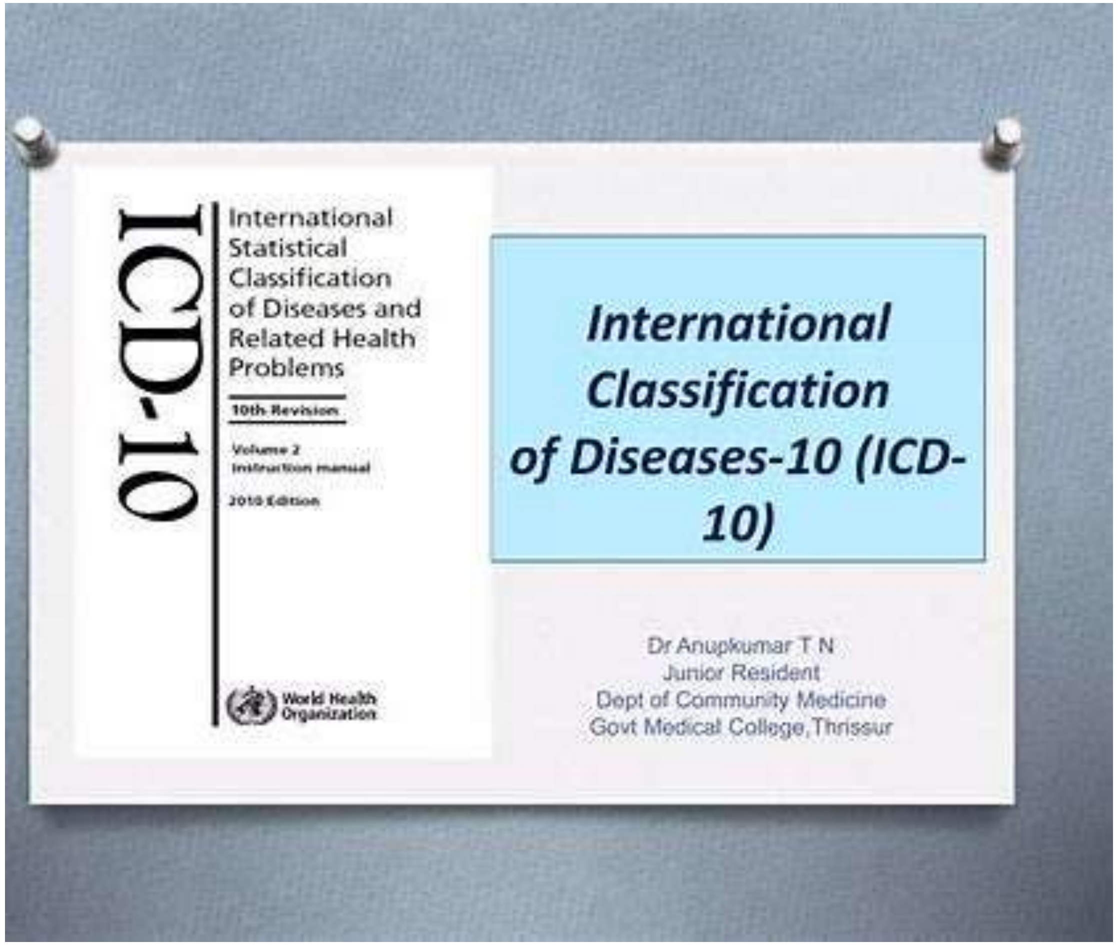
Interoperability Vocabularies

- Standardized definitions from publicly available value sets and coding vocabularies
- Provide shared understanding and meaning to the user
- Examples:
  - Snomed – Systemized Nomenclature of Medicine
    - Example: heart attack, myocardial infarction
  - WHODRUG – international drug dictionary
    - Example: Panadol, Tylenol, Efferalgan, Paracetamol
  - CPT – Current Procedural Terminology
    - Example: Surgery, anesthesia, blood drawing, physical therapy

SNOMED CT

The global
language of
healthcare

Interoperability Vocabularies



ICD-10

International Statistical Classification of Diseases and Related Health Problems

10th Revision

Volume 2
Instruction manual

2010 Edition

World Health Organization

International Classification of Diseases-10 (ICD-10)

Dr Anupkumar T N
Junior Resident
Dept of Community Medicine
Govt Medical College, Thrissur

Example: Loss of consciousness, headache, concussion, traumatic brain injury

Interoperability Solutions

- In the U.S. **TEFCA**, the Trusted Exchange Framework and Common Agreement (Version: 2.0 April 2024), outlines a common set of principles, terms, and conditions to enable nationwide exchange of electronic health information across disparate health information networks.
- https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement
- Goals:
  - to establish a universal governance, policy, and technical floor for nationwide interoperability;
  - to simplify connectivity for organizations to securely exchange information to improve patient care, enhance the welfare of populations, and generate health care value; and
  - to enable individuals to gather their health care information.
- https://www.mobihealthnews.com/video/tefca-and-health-data-exchange-2024

Interoperability Examples

- Can the laboratory system download values into the electronic medical record?
- Can a patient’s MRI scan be reviewed by a physician in another city?
- Can the pharmacist send a prescription to a drug store in another region?
- Can the data from a mobile device used at home be collected by an electronic medical record?

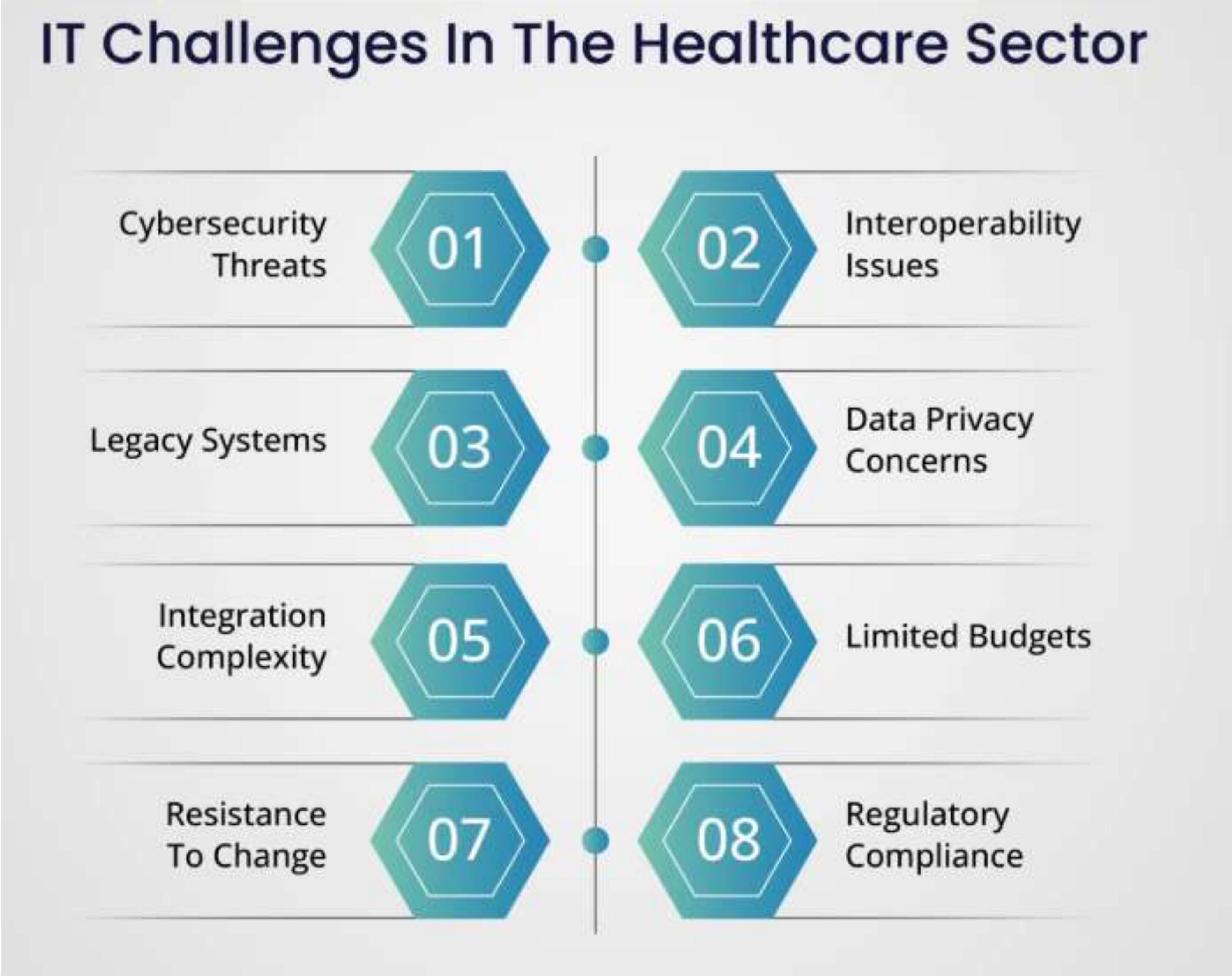
Interconnectivity

Interconnectivity Definition

- All parts of a system interact with and rely on one another.
- Connectivity means devices communicating and making it possible to transport or receive data. However, the focus is on collecting information more than integrating it.
- Connectivity is a low level of interoperability, sometimes the terms are used interchangeably.

Interconnectivity Examples

- Devices, for example infusion pumps, ventilators, blood pressure monitors and other vital sign monitors connected to the EMR
- Are medical supplies used by the patient linked to the hospital billing system?
- Goal: Reduce human error in reporting and communications



IT Challenges In The Healthcare Sector

01 Cybersecurity Threats

02 Interoperability Issues

03 Legacy Systems

04 Data Privacy Concerns

05 Integration Complexity

06 Limited Budgets

07 Resistance To Change

08 Regulatory Compliance

Confidentiality

Confidentiality Definition

- Confidentiality refers to protection of information shared with a physician, therapist or attorney from being shared with others without express consent.
  - During a dialogue in a medical visit, a patient can reveal information confidentially.
- A patient can trust his/her physician to not share personal information regarding his/her health, home, or lifestyle habits discussed in candid conversation.
- Confidentiality is rooted in ethics.

Confidentiality

- Information a patient tells a physician must be kept private
  - Exceptions: transferring information to other health providers; e.g. a pharmacist, who needs to fill a prescription, or a technician taking an x-ray.

- Confidentiality is important for respect of patients and to encourage honest, open conversations between patients and physicians.

- Personal information revealed during doctor visits adds to the understanding of a patient’s case, ongoing health, and prognoses.

Privacy

Privacy Definition

- Privacy is the **legal protection** of patient records, prescriptions, and examinations from being shared or accessed by anyone other than his/her physician.
- Privacy keeps medical records legally bound from public release but they can become available to third parties (for research purposes), but those records cannot be tied to specific patients.

Privacy Standards

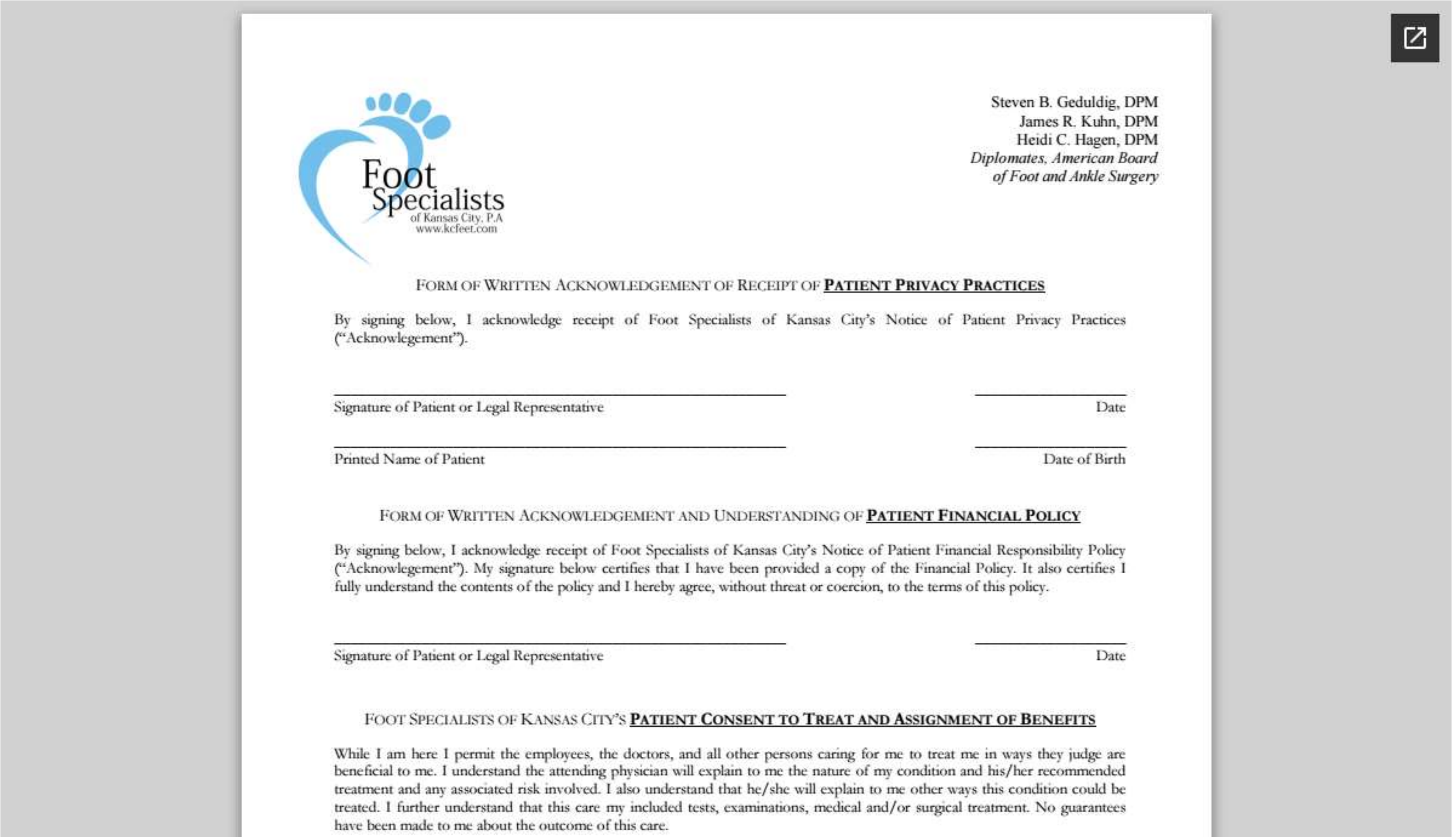
- The European Union General Data Protection Regulation (GDPR) went into effect in 2018, an extremely strong privacy and security law.
- **Healthcare organizations who treat patients from any of the 28 EU nations need to comply with the law.**
- GDPR requires companies to gain affirmative consent for any data collected from people who reside in the EU.
- Providers will need to consider personal data (eg, photos) data flows, cross-border data transfer, and security monitoring, to ensure their policies are compliant with the law.
- Fines are significant.

Privacy Standards

- In the U. S., health care providers must follow the **Health Insurance Portability and Accountability Act (HIPAA),** a privacy rule that federally restricts personal health information from being disclosed as a public record.
- According to HIPAA, patients must sign a form acknowledging how their information will be shared.
- In the U.S., if personal medical information reveals patient identity and it reaches an unauthorized third party without patient consent, the patient has the right to take legal action.

Privacy

In the U.S., patients sign a HIPAA form for every encounter and indicate if they want their information shared, like this one below



Foot Specialists
of Kansas City, P.A
www.kcfeet.com

Steven B. Geduldig, DPM
James R. Kuhn, DPM
Heidi C. Hagen, DPM
Diplomates, American Board
of Foot and Ankle Surgery

FORM OF WRITTEN ACKNOWLEDGEMENT OF RECEIPT OF **PATIENT PRIVACY PRACTICES**

By signing below, I acknowledge receipt of Foot Specialists of Kansas City's Notice of Patient Privacy Practices ("Acknowlegement").

____________________________________ ____________
Signature of Patient or Legal Representative Date

____________________________________ ____________
Printed Name of Patient Date of Birth

FORM OF WRITTEN ACKNOWLEDGEMENT AND UNDERSTANDING OF **PATIENT FINANCIAL POLICY**

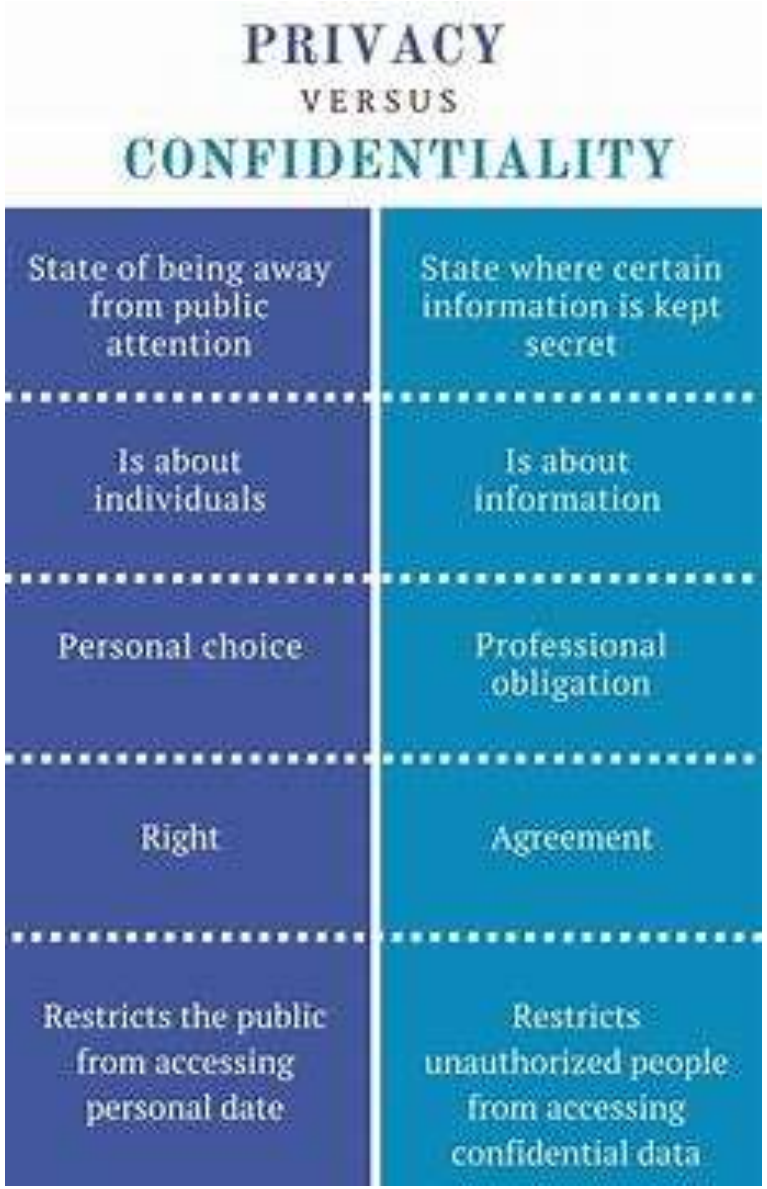
By signing below, I acknowledge receipt of Foot Specialists of Kansas City's Notice of Patient Financial Responsibility Policy ("Acknowlegement"). My signature below certifies that I have been provided a copy of the Financial Policy. It also certifies I fully understand the contents of the policy and I hereby agree, without threat or coercion, to the terms of this policy.

____________________________________ ____________
Signature of Patient or Legal Representative Date

FOOT SPECIALISTS OF KANSAS CITY'S **PATIENT CONSENT TO TREAT AND ASSIGNMENT OF BENEFITS**

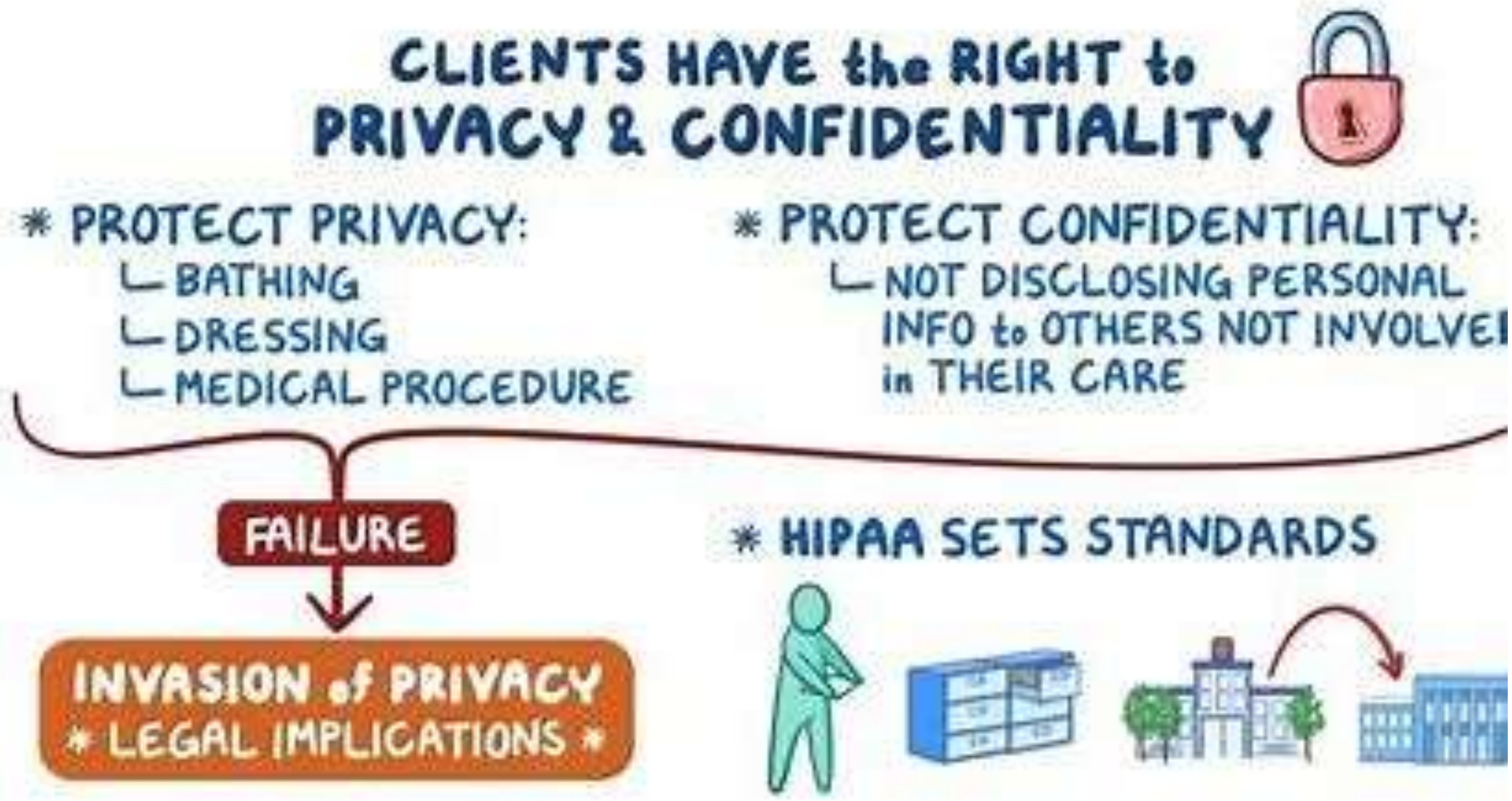
While I am here I permit the employees, the doctors, and all other persons caring for me to treat me in ways they judge are beneficial to me. I understand the attending physician will explain to me the nature of my condition and his/her recommended treatment and any associated risk involved. I also understand that he/she will explain to me other ways this condition could be treated. I further understand that this care my included tests, examinations, medical and/or surgical treatment. No guarantees have been made to me about the outcome of this care.

- Confidentiality and privacy are not the same!



PRIVACY
VERSUS
CONFIDENTIALITY

State of being away from public attention	State where certain information is kept secret
Is about individuals	Is about information
Personal choice	Professional obligation
Right	Agreement
Restricts the public from accessing personal date	Restricts unauthorized people from accessing confidential data



CLIENTS HAVE the RIGHT to PRIVACY & CONFIDENTIALITY

- PROTECT PRIVACY:
  - BATHING
  - DRESSING
  - MEDICAL PROCEDURE

- PROTECT CONFIDENTIALITY:
  - NOT DISCLOSING PERSONAL INFO to OTHERS NOT INVOLVE in THEIR CARE

FAILURE → INVASION of PRIVACY

* LEGAL IMPLICATIONS *

- HIPAA SETS STANDARDS

Confidentiality and Privacy in Spain

- Spain has laws that regulate patient autonomy and data protection, including the Spanish Law on Patient Autonomy, known as the **Patients' Rights Law (PRL).**
- This law requires that personal identification data, such as a Social Security number or ID card, be separate from health data.
- Information with the patient's consent can be used for scientific research, for judicial inquiries, and for public health risk.

Confidentiality and Privacy: Discussion Questions

- In a hospital elevator, a nurse is talking to another nurse about a patient’s symptoms. Is this a breach of privacy?
- A pharmaceutical company wants data to understand whether treatment is effective. It receives data from a clinic, is it enough to blind the data from personal identification?
- A medical student accesses a government health database. How can he or she use the data for research complying with privacy and confidentiality?

Confidentiality and Privacy

- Check out the privacy concerns related to Google and Deep Mind and the NHS in the U.K.
- DeepMind, a London artificial intelligence lab with a focus on neural networks, acquired by Google, was developing a patient monitoring app called Streams using NHS patient data
- In 2016, the U.K.'s National Health Service gave them access to pseudonymized data from 1 million patients without consent
- Legal action followed.
- https://www.cnbc.com/2021/10/01/google-deepmind-face-lawsuit-over-data-deal-with-britains-nhs.html

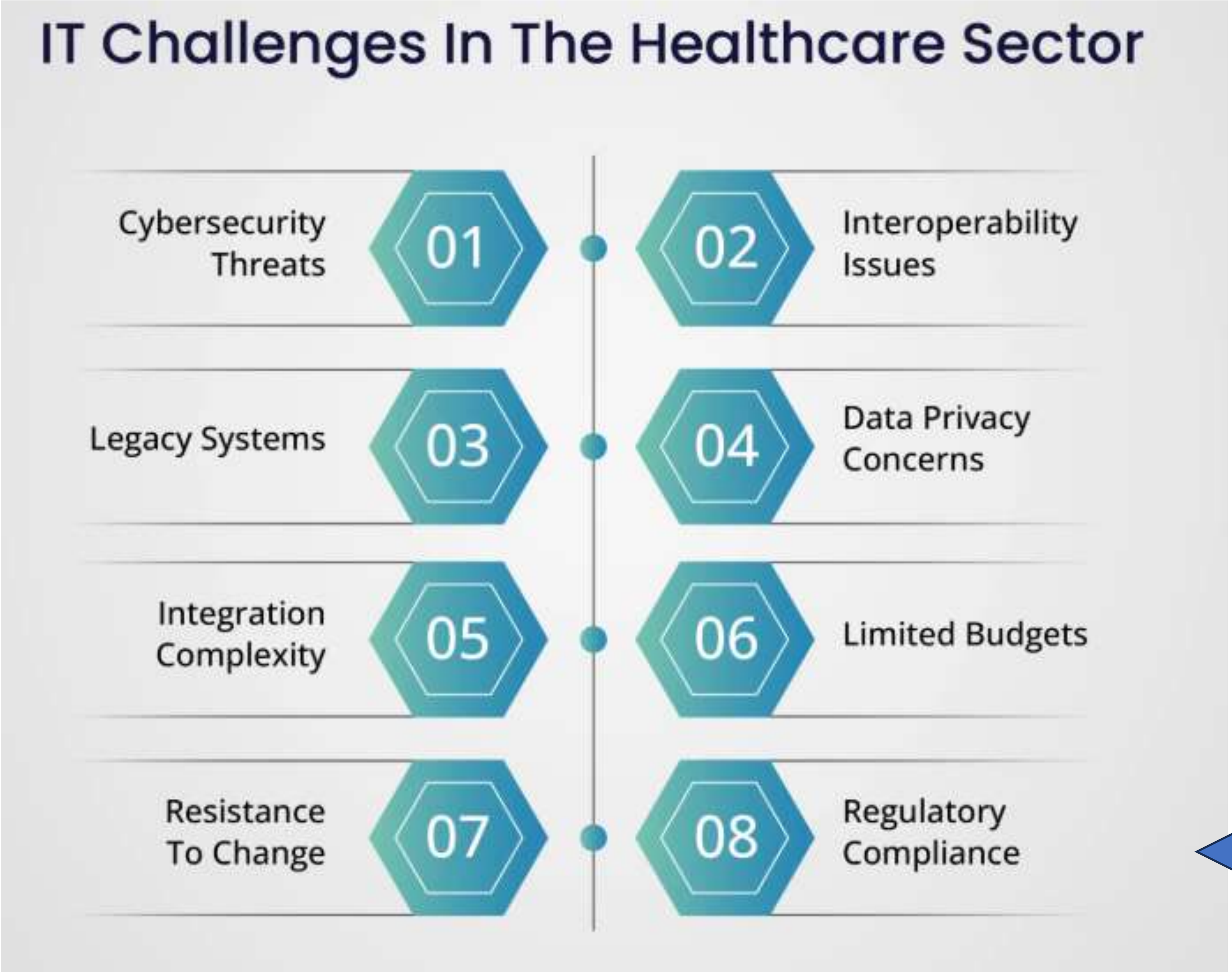
Google DeepMind

Confidentiality and Privacy

- Check out the grab for patient data
- In 2019. the British *Guardian* published an account from an anonymous whistleblower at Project Nightingale at Google, accusing the company of misconduct in regard to handling sensitive health data.
- Data from 50 million patients. had not been anonymized nor were the doctors notified or consent given by patients.
- Google employees had full access to non-anonymous patient health data.

- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7059004

- What happened to privacy and confidentiality?
- Need for data science ethics review



IT Challenges In The Healthcare Sector

01 Cybersecurity Threats

02 Interoperability Issues

03 Legacy Systems

04 Data Privacy Concerns

05 Integration Complexity

06 Limited Budgets

07 Resistance To Change

08 Regulatory Compliance

Other challenges: Ethics and governance

Data ownership, data stewardship

Ethics in medicine

DO NO HARM!

- Moral principles that apply values to the practice of medicine, biomedical research, and now in digital health, clinical data, AI and so on.
- In 2016, Stephen Hawking, the English theoretical physicist said that the creation of AI might be not the best but the worst thing for the mankind.

Ethical Challenges in Digital Health and AI

- Example:
- A newborn baby is in the neonatal ICU for surgery for a diaphragmatic hernia.
- The AI settings on the mechanical ventilator suggest increasing the level of oxygen.
- The respiratory therapist warns that high concentrations of oxygen in a baby could make the baby go blind.
- Who does the nurse listen to?

Ethical Challenges in Digital Health and AI

- Example: A doctor has access to the medication profile of a young patient (22 years old) prescribed Abilify (the smart pill) for bipolar disorder. She notices that the digital record shows she has not been taking the drug. She is now having a manic episode.
- Should the doctor call her parents? Should the doctor force treatment in the emergency department? Will the doctor obtain written consent for treatment? How will people in the community be protected from possible harm?
- Sticking to a medication regimen is important for people with mental illness but digital tracking raises ethical issues.

Ethical challenges in Digital Health and AI

- Trust and transparency
  - High risk decision making.
    - Think about implanting brain-computer interfaces
    - Think about cardiac pacemakers
- Bias
  - Data collection and algorithm development can perpetuate healthcare disparities
    - Are all groups considered in training the model? For example, women, disabled
- Equity
  - Address inequalities and promote diversity in AI research and the workforce
- Responsibility
  - Get many perspectives in decision making from doctors, nurses, policy makers, patients, biomedical engineers, ethicists, lawyers to ensure equitable outcomes

- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10492220/

Ethics Discussion Questions

- Will there be a backlash against technology if ethical concerns are not addressed in advance?

- How and who should resolve the ethical issues?
  - Informed consent, autonomy, data ownership, access and fairness?

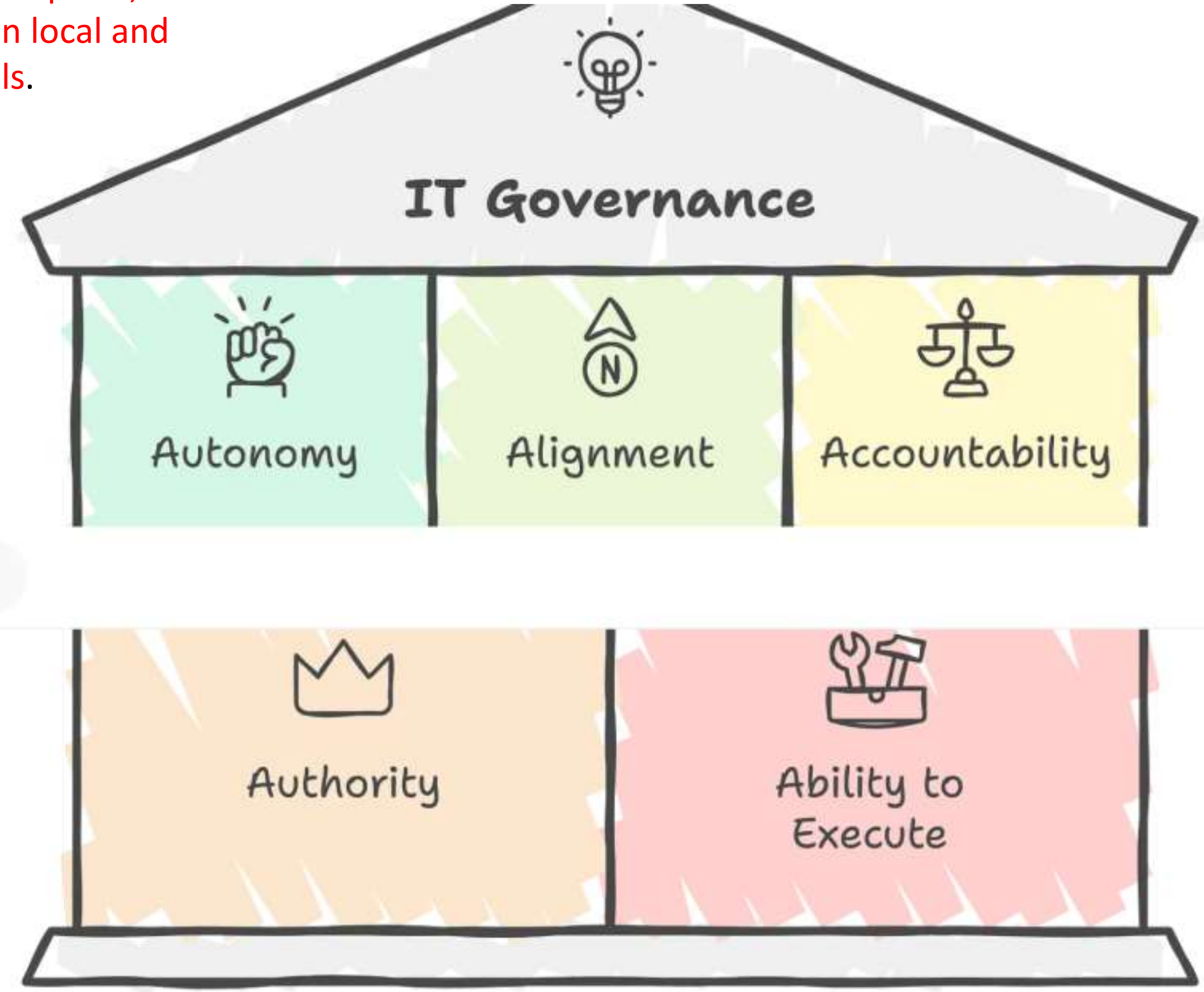
- What should be the rights of patients when their data is included in huge datasets?

- Read: Nature Electronics (2019, August) Time to Switch on to Digital Ethics. https://www.nature.com/articles/s41928-019-0299-x
- Read: Gerke, S. (2019, August) More challenges in digital health. Ethical and Legal Issues of Ingestible Electronic Sensors. https://www.nature.com/articles/s41928-019-0290-6.pdf?origin=ppub

Governance in Health IT

- What is it?
- Organization-wide, accountability framework that promotes appropriate behavior when handling health information.
- Includes the processes, rules, standards and criteria to ensure the use of information helps to achieve the organization's goals
- Includes how information is created, stored, used, archived and discarded.
- Determines who should have access to what data, when and how.

For clinics, hospitals, health ministries on local and federal levels.



Governance in Health IT

- Examples: Project management, aligning clinical and business priorities, risk management, cost control and regulatory and quality compliance.
- Typical questions for Governance:
  - Are our IT strategies, processes, and initiatives aligned with the goals of the organization?
  - Are we investing in the right IT projects at the right time-not too soon, not too late-to ensure that our organization is successful?

Challenges in Digital Health

Cybersecurity
Confidentiality
Privacy
Interoperability
Interconnectivity
Ethics
Governance

Should patients be compensated for data breaches when their info is compromised?

Who wins - the doctor’s decision or the algorithm?

Is social monitoring for health OK?

Should a machine make independent decisions about a person’s health?

Can digital health reduce inequalities?

And finally, what moral values – human, social, economic – should be fundamental, regardless of the technologic innovation?

Next session:

Health informatics – data analytics, decision support, business intelligence

- Happy Semana Santa