

Cybersecurity meets patient health impacts

A framework for characterising
cyber incidents
in healthcare settings

11th eHealth Security Conference

07 October 2026 Nicosia

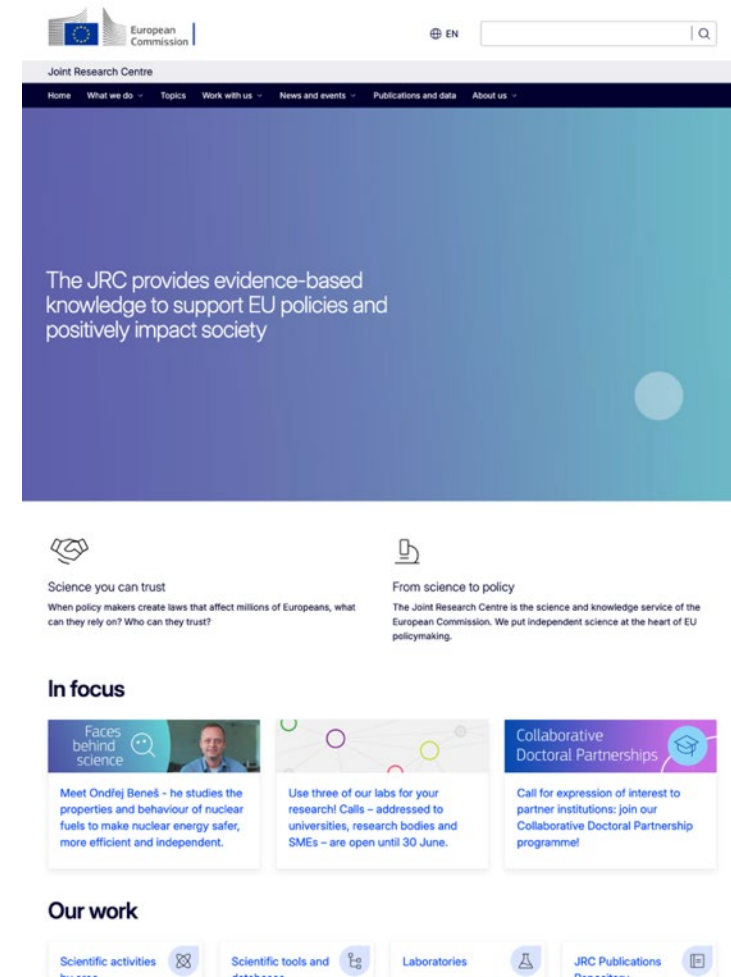
Vittorio Reina & Claudius B. Griesinger*

Acknowledgements: Diego Dall'Alba

European Commission – DG JRC

Joint Research Centre

- **Scientific service of the Commission**
- **Large horizontal service**
- **No policy agenda**
- **Key role**
Creating and interpreting evidence for various EU policies



https://joint-research-centre.ec.europa.eu/index_en



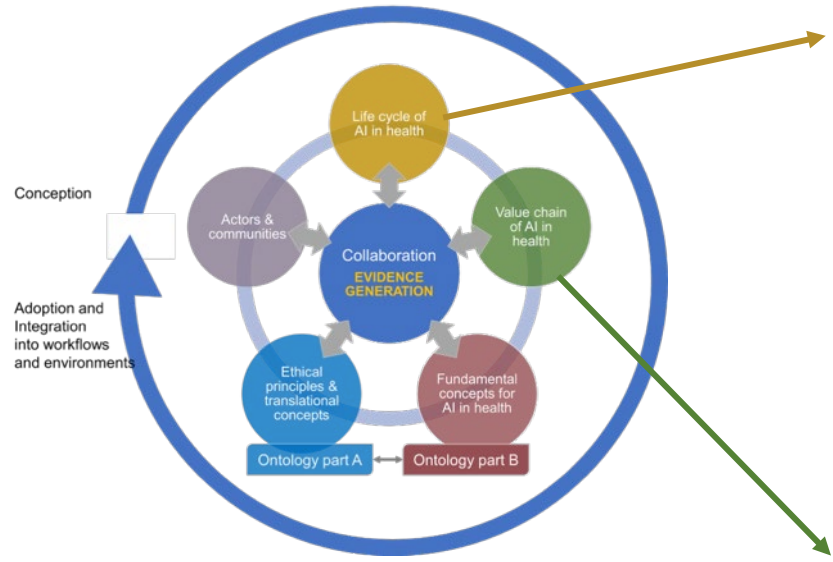
1

The importance of cybersecurity for health digitisation



Cybersecurity: preserving value & ensuring patient safety

AI evidence pathway for health



Cybersecurity in digital healthcare:

- Value chain element: **value preserving enabler**
- A concern for **patient safety**



Trust: key for investors

Innovation

Adoption &
Integration

J.P.Morgan
ASSET MANAGEMENT

Products Investment Strategies Ir

Sustainable investing insights

Trust in AI: A critical consideration for investors



Artificial intelligence has dominated markets and investor attention, with US large-cap AI funds to record highs and three consecutive years of 15%+ total returns from 2023 through year-end. The sector is characterized by investment in physical infrastructure and capital expenditure. However, investors are shifting towards intangible factors like trust as a central driver of long-term opportunity.

Identifying the next generation of winning AI companies will therefore require a greater focus on trust. To integrate and scale Gen AI while concurrently trying to preserve and build trust with employees. This balancing act will have implications for technology companies, AI infrastructure providers, and the AI value chain.

Rather than focusing on infrastructure and capex, key issues for investors now include user acceptance, regulatory compliance, and stakeholder engagement:

- **User safety and data integrity are central to building consumer trust.** High-profile incidents and regulatory actions underscore the importance of robust guardrails, transparency, and responsible governance in AI product development.
- **Community opposition and regulatory hurdles are slowing AI infrastructure expansion.** Data center projects face increasing delays and cancellations due to concerns over electricity costs, water usage, and other local impacts, with continued scrutiny.

Cybersecurity:
security of data, assets, operations &
safety of patients
is key for **trustworthiness** of
digital health solutions



2

Cyber incidents in health (CIH)

- a growing public health problem



Cyber incidents in health (CIH) are on the rise

Digitisation of healthcare critical to tackle challenges

- Hyperaging (e.g. EU, China...)
- Health worker shortage
- Personalisation of medicine: integration of multimodal data

Digitisation creates new „attack surfaces“

- Internet of things (IoT), connected devices, wearables
- “Artificial Intelligence”: machine learning, expert systems etc.
 - Discriminative models, e.g. diagnostic tools
 - Generative models: models trained on data distributions (e.g. LLMs, multimodal models)
- Cloud data storage and cloud computing
- Varied use environments, e.g. hospitals versus home care (telemedicine)
- Electronic health records -> European Health Data Space (EHDS)

Health sector-specific challenges

- Broad spectrum of entities and actors
- Insufficient funding for security @ organisations
- Technical security hurdles, e.g. legacy devices



Image: <https://tedismedical.com/en/cyberattacks-in-the-healthcare-sector/>

Cyber incidents in health (CIH) and patient safety

Cybersecurity in Healthcare: New Threat to Patient Safety

Bakheet Aldosari ¹

1. Health Informatics, King Saud Bin Abdulaziz University for Health Sciences, Riyadh, SAU

Corresponding author: Bakheet Aldosari, dosarib@gmail.com

- Cyberattacks frequently disrupt healthcare operations
- critical systems, medical devices, and communication networks inoperable.
- Paralysis of hospital workflows: patient care delivery delayed, emergency services compromised, clinical decision-making undermined -> **patient safety at risk**

Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients

Hannah Neprash

Claire McGlave

Sayeh Nikpay

AMERICAN ECONOMIC JOURNAL: ECONOMIC POLICY
VOL. 18, NO. 1, FEBRUARY 2026
(pp. 256–81)

- Created database of hospital ransomware attacks to Medicare claims data.
- Quantification of effects of ransomware attacks on hospital operations and patient outcomes.
- Hospital volume decrease by 17–24 % during 1st week of attack
- Recovery within within 3 weeks
- Among patients already admitted to the hospital when attack occurred, **in-hospital mortality increases by 34–38 percent.**



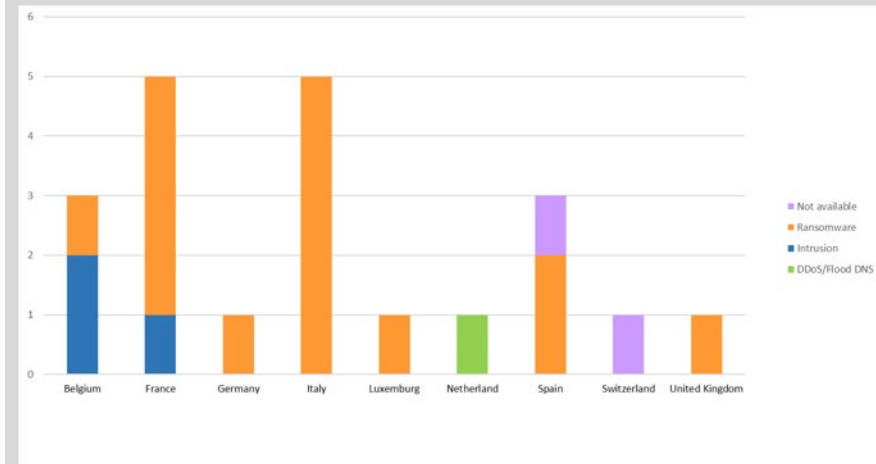
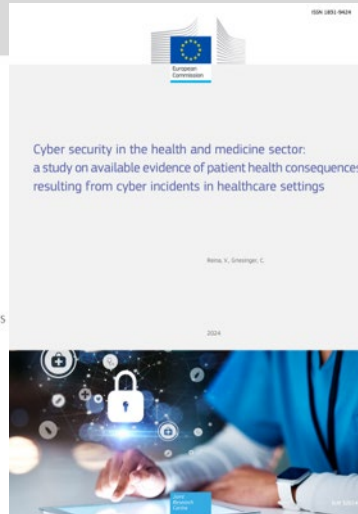
Cyber incidents in health (CIH) within the EU



ENISA threat landscape – health 2023

- 215 CIHs across European health organizations (January 2021 to March 2023)
- **data collection mechanisms were insufficient to assess the exact consequences of delayed treatment and care for patient's health.**

„... we cannot measure accurately the impact of delayed treatment and care to a patient's health, and we rely on related estimated projections.“



JRC report 2024

- Monitoring CIH over one year: May 2022-April 2023
- Information published in EN, IT, FR, ES, DE
- **21 incidents: mainly ransomware**
- **Health impacts**

European Commission, Joint Research Centre, Reina, V. and Griesinger, C., Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Publications Office of the European Union, Luxembourg, 2024, <https://data.europa.eu/doi/10.2760/693487>, JRC13869

3

Effective responses
require a meaningful
CIH characterisation



2025 EU action plan on cybersecurity of hospitals and healthcare providers

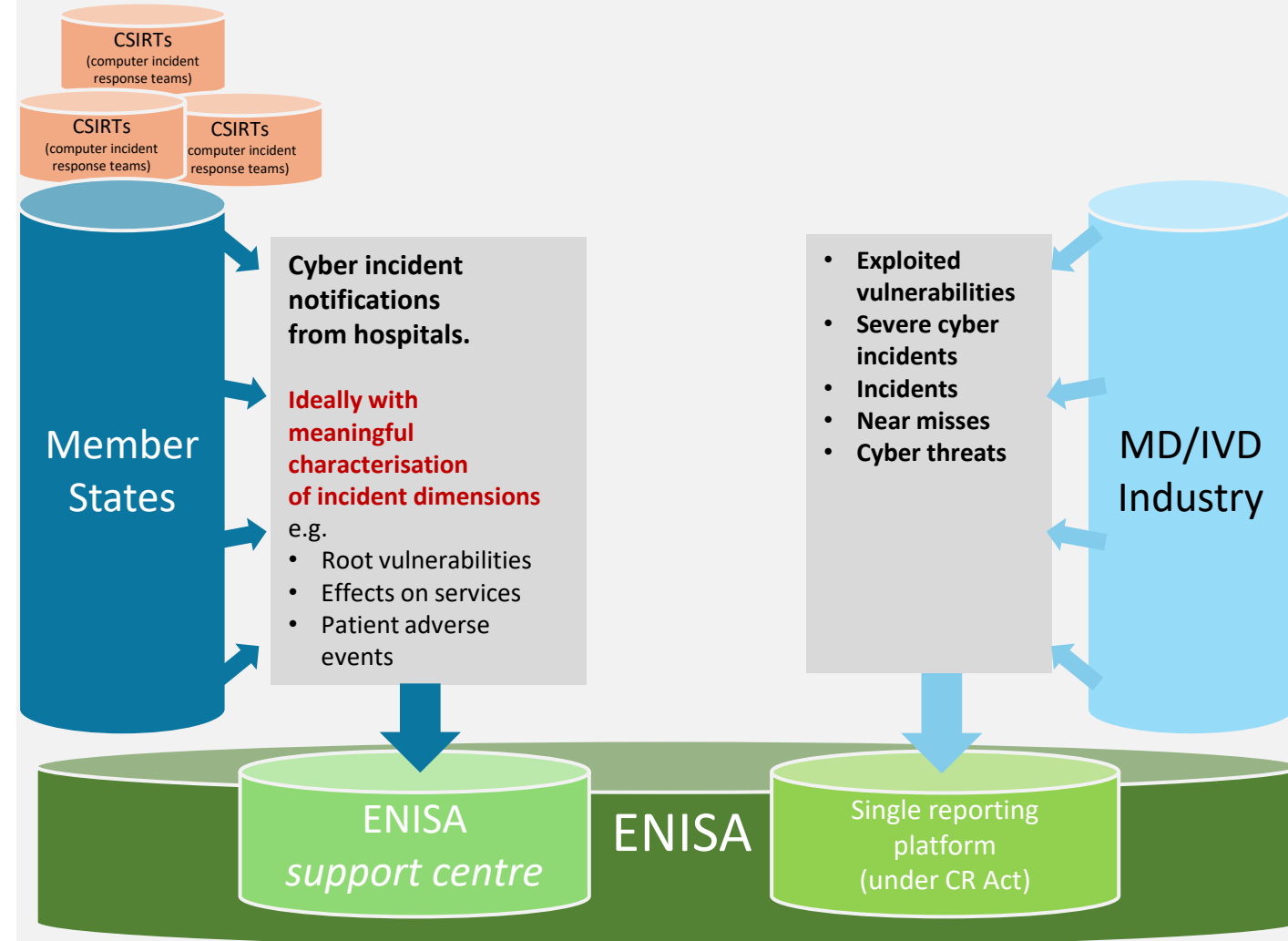
Structuring available knowledge & tools

ENISA

European cybersecurity support centre for hospitals and healthcare providers

- **Develop service catalogue**
 - Preparedness/prevention
 - Detection
 - Response & recovery
- **Develop repository of available instruments** at EU, national, regional level.
Work with MS, draw on knowledge at local level.
- **Pilots to develop best practices**
 - Cyber hygiene
 - Security risk assessment
 - Cybersecurity monitoring
 - Threat intelligence
 - Incident response using state of the art solutions

Reporting & characterisation



Characterising CIH: the challenges

General evidence gap

Although **accurate characterisation & description of cyber events is critical for effective responses** (NIST, 2025) there remains an **evidence gap concerning CIH** and, in particular, patient effects

Reasons include

- Fragmented reporting obligations
- Lack of mandatory disclosure requirements
- Numerous frameworks and taxonomies but
 - Different terminology
 - No alignment reg. categorisation of properties
 - Typically not focused on health

Particular challenge:
patient effects,
especially delayed ones



Immediate effects can be directly observed (e.g., reduction in laboratory and diagnostic capabilities), while the **potential downstream consequences of care disruptions and delays on patient outcomes** are considerably more difficult to quantify objectively.

- Abbou B, Kessel B, Ben Natan M, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. *Front Digit Health*; 6. Epub ahead of print 16 February 2024. DOI: 10.3389/fdgth.2024.1321485.
- Keogh RJ, Harvey H, Brady C, et al. Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. *Journal of Cancer Policy* 2024; 39: 100466

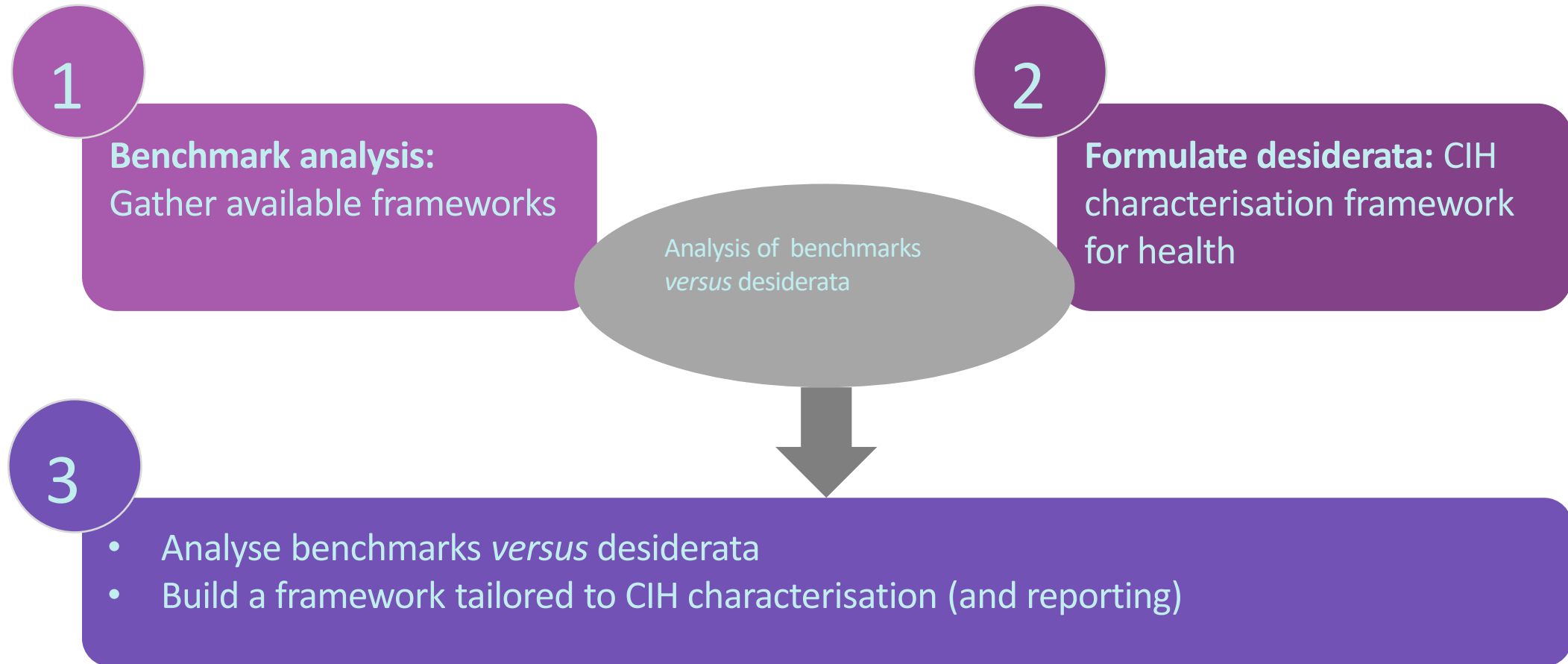
There is a remarkable **lack of quantitative data on the impact of downtime on healthcare systems and patient health** despite the increasing rate of occurrence of these events.

- Larsen EP, Rao AH, Sasangohar F. Understanding the scope of downtime threats: A scoping review of downtime-focused literature and news media. *Health Informatics J* 2020; 26: 2660–2672

4

JRC framework for characterising CIH

Our approach for building a framework for CIH characterisation



Benchmarks & Desiderata

19 benchmark documents analysed

Reference	Title	Author	Year
25	Incident Response Recommendations and Considerations for Cybersecurity Risk Management (NIST)	Nelson et al.	2025
37	Recommendations of the National Institute of Standards and Technology (NIST)	Cichonski et. al	2012
38	UK cyber security - The role of insurance in managing and mitigating the risk	U.K. Government and Marsh	2015
28	National cyber incident scoring system	U.S. Cybersecurity and Infrastructure Security Agency (CISA)	2020
39	Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response	ISO/IEC	2023
40	A FAIR Taxonomy for Cyber Risk Scenarios	Goyal et al.	2025
33	The ACN cyber taxonomy	Italian National Cybersecurity Agency (ACN)	2024
41	Reference Incident Classification Taxonomy	European Union Agency for Network and Information Security (ENISA)	2018
42	Malware Information Sharing Platform (MISP)	Andras Iklody (lead developer) and other contributors	June 2025 current version
43	MITRE ATT&CK®	MITRE Corporation	Apr. 2026 current version
44	Vocabulary for Event Recording and Incident Sharing (VERIS)	VERIZON	
45	Cyber incident reporting framework: global edition	Cyber Threat Alliance (CTA) and the Institute for Security and Technology (IST)	2023
46	Cyber-attack classification scale methodology	European Network of Transmission System Operators for Electricity (ENTSO-E) and European Distribution System Operators' Entity (EU DSO)	2025
47	Assessing resilience of hospitals to cyber-attack	Ghayoomi et al.	2021
48	A cyber risk assessment approach to federated identity management framework-based digital healthcare system	Huda et al.	2024
49	The cybersecurity and the care robots: a viewpoint on the open problems and the perspectives	Giansanti and Gulino	2021
50	A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate	Agrafiotis et al.	2018
51	Effective metrics to detect and prioritize cyber incidents in healthcare	Alexander and Wang	2025
52	Examining the costs and causes of cyber incidents	Romanosky	2016

Desiderata

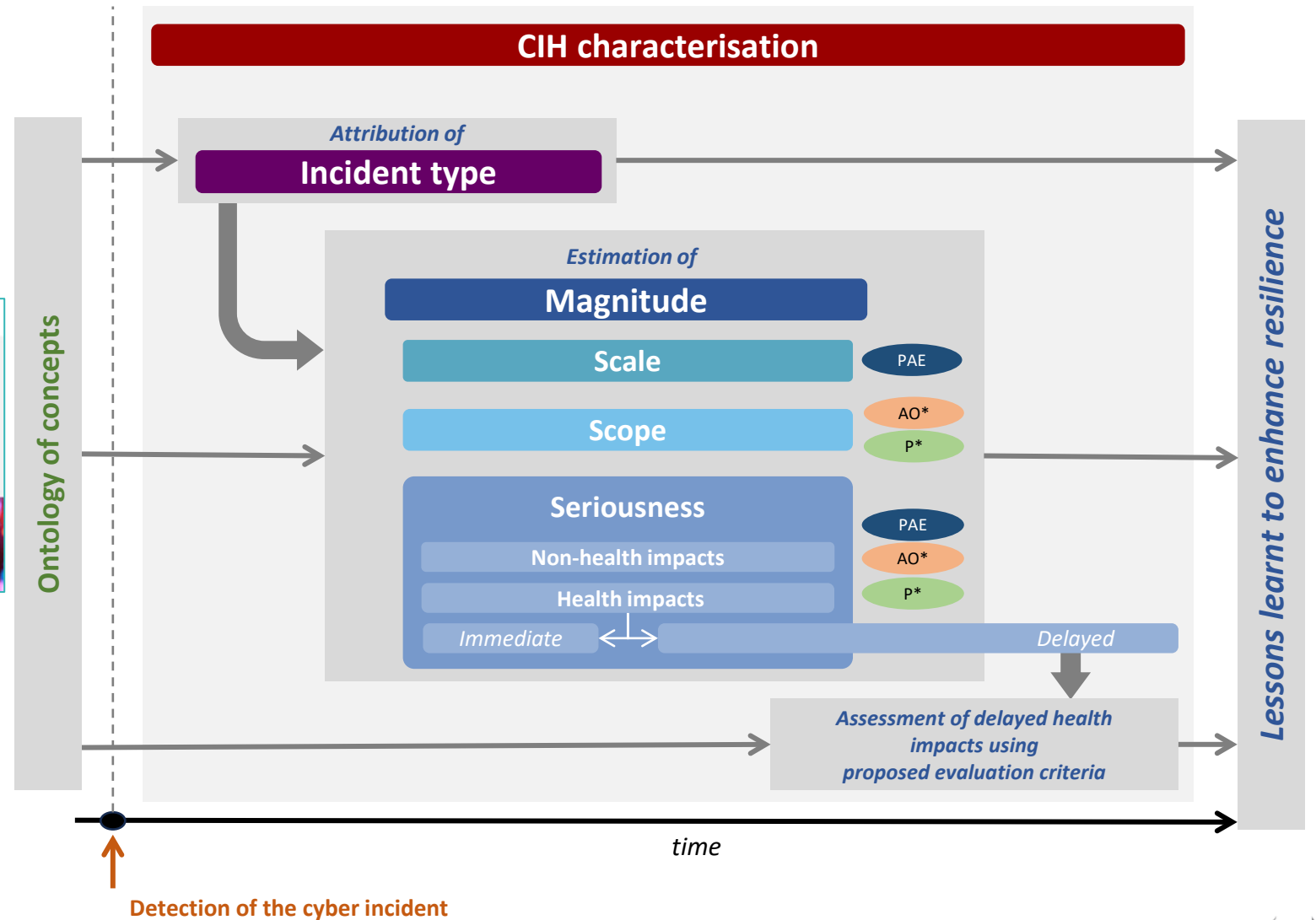
- 1. Sound conceptual foundation:**
based on unambiguous concepts
- 2. Health-sector specificity**
- 3. Comprehensiveness** regarding damage characterisation
- 4. Supporting both attack type and threat actor characterisation**
- 5. Supporting temporal dimension analysis**
- 6. Supporting geographical dimension analysis**
- 7. Distinguishing impacts on**
natural persons versus organisation level
- 8. Supporting impact analysis** on IT infrastructure and data
- 9. Supporting impact analysis** on health-relevant services
- 10. Supporting analysis of potential association**
with (delayed) health impacts in patients



Characterisation framework of CIH

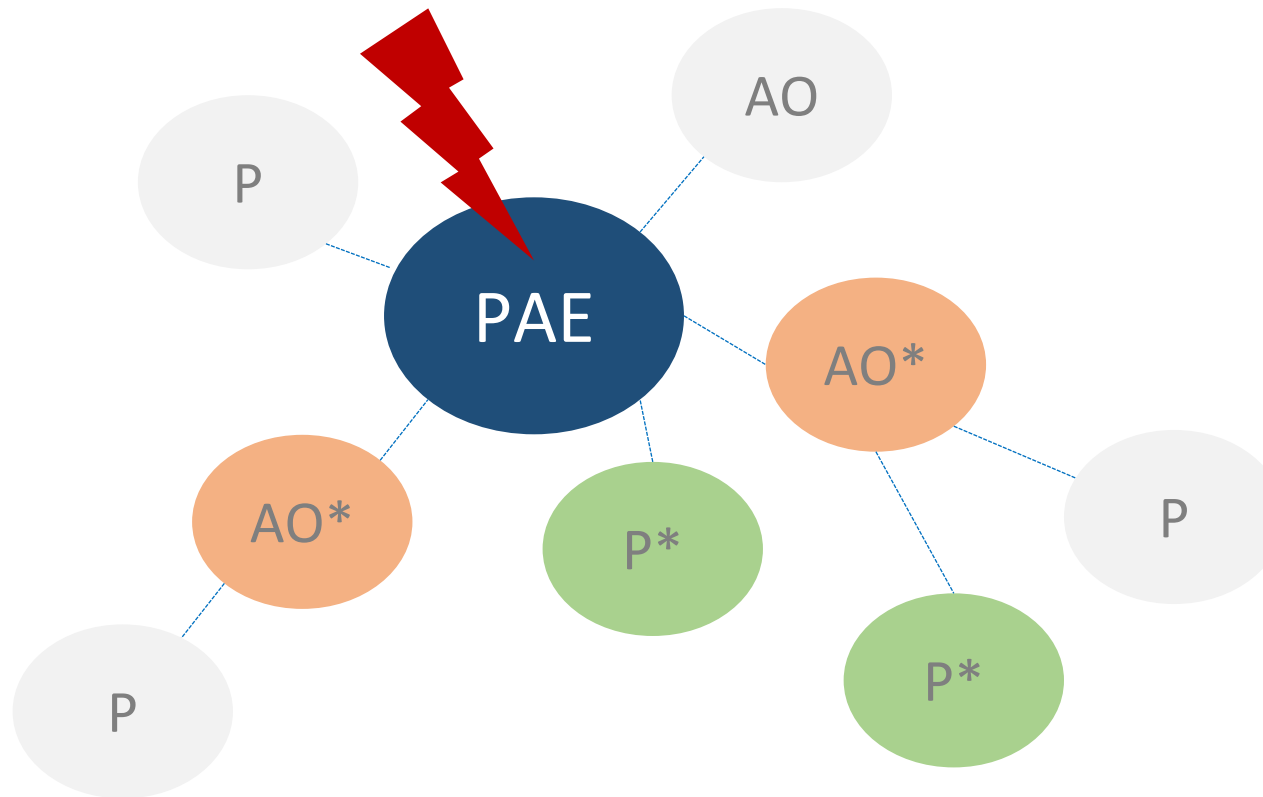
70 concepts grouped in four categories:

- **Cybersecurity:** key concepts of cybersecurity, e.g. threats, vulnerabilities, attacks, incidents.
- **Enabling IT infrastructure:** components necessary to operate and manage IT environments of organisations (e.g. IT hardware, computer software, network and storage infrastructure)
- **Enabling technologies:** platforms and applications employed for the development, implementation and operation of AI systems (e.g. containerization and virtualization solutions, data pipelining, libraries)
- **Health impacts:** set of relevant health impacts that may result from cyber incidents (e.g. delay to treatment/therapy, death, hospitalisation or prolonged hospitalisation, disruption of medical procedures)



Entities and individuals affected by a cyber incident: D6 geographical analysis + D7

Cyber incident



PAE = primary affected entity

AO = associated organisation
(stakeholder of PAE)

P = person / patient affected
(directly at PAE or at AO)

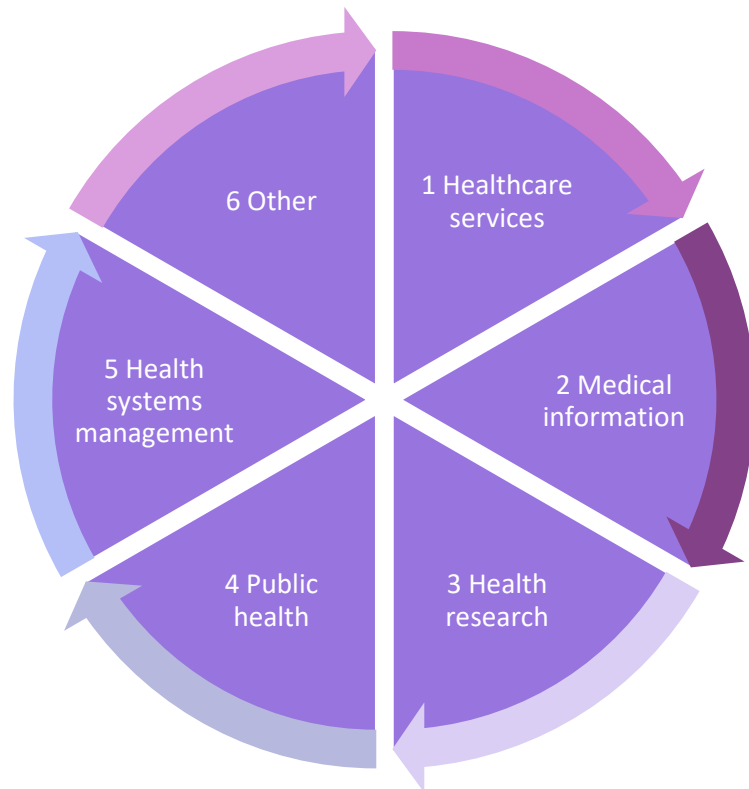
Types of cyber incidents targeting the health sector

Attribution of

Incident type

6 types:

- 4 WHO health application domains
- 1 Medical information
- 1 other



Healthcare services

- CIH-1: Incident compromising availability and/or integrity of healthcare services, including critical

Medical information

- CIH-2: Incident involving, specifically, electronic health records (EHR) / medical records of patients
- CIH-3: Incident leading to leaks of private, personal or otherwise confidential information including circumscribed medical information

Health research

- CIH-4: Incident compromising availability and/or integrity of systems for health research

Public health

- CIH-5: Incident compromising availability and/or integrity of systems for public health surveillance
- CIH-6: Incident involving, specifically, the gathering, processing and making available of critical public health information

Health systems management and planning

- CIH-7: Incident compromising availability and/or integrity of health systems management and planning Supply chain(s)
- CIH-8: Incident involving critical supply chains and availability of health products/services

Other

- CIH-9: Incident types not captured by any of the previous types

Estimation of cyber incident magnitude: 3S dimensions

Magnitude

Scale

Primary affected entity

Duration and time to recovery

Confidential business information

IT systems

Attack and threat actors

Scale: the extent and severity of negative impacts at the PAE targeted by the attack (e.g. a provider of cloud storage solutions, a company developing AI systems, a hospital)

Scope

Associated organisations

Patients

Geographical spread

Services unavailable/compromised

Scope: the “breadth” or “latitude” of the incident impact when looking at stakeholders of PAE such as AO and/or affected person/patient (P) directly at PAE or at AO

Seriousness

Non-health impacts

Affected services

Confidential information, personal or private data

Financial and socioeconomic impacts

Health impacts

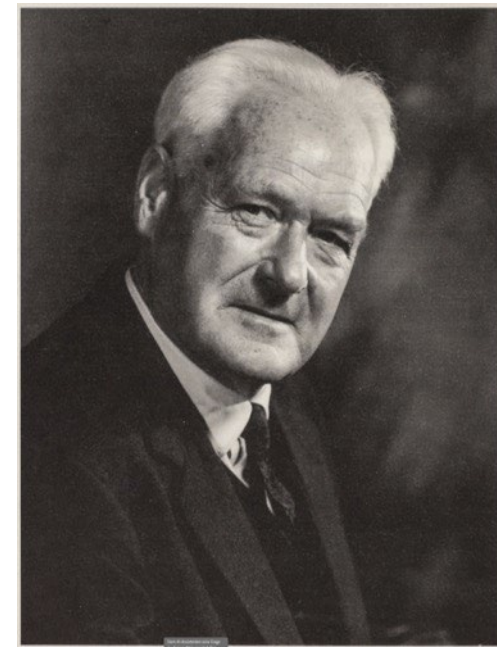
Immediate health impacts

Delayed health impacts

Seriousness: the gravity of adverse impacts/damages experienced by PAE, AO and P

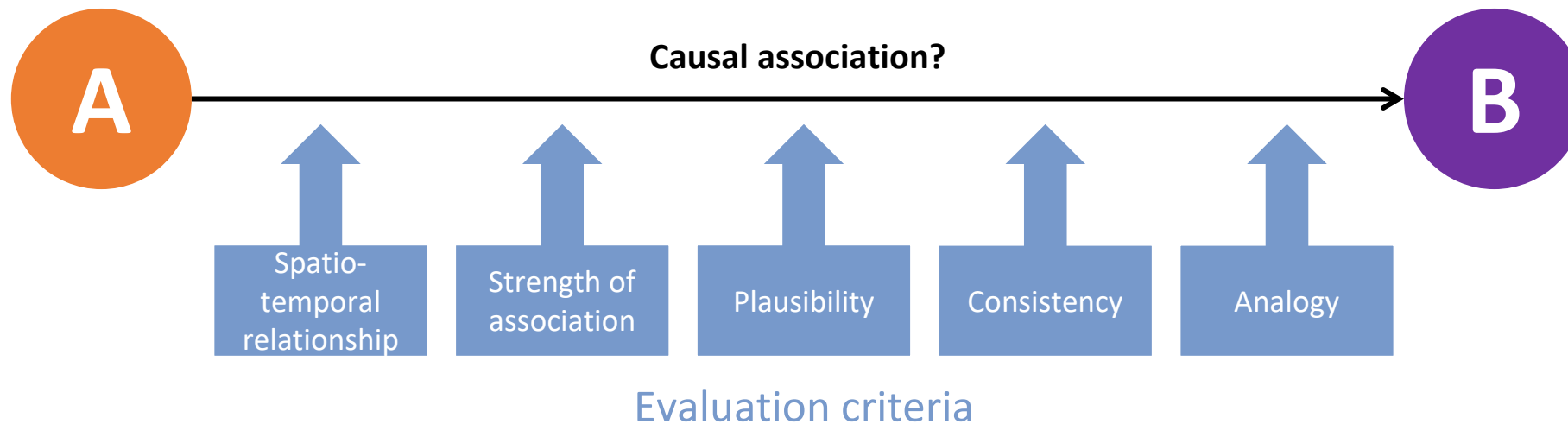
Assessment of delayed health impacts

Five criteria based on the **Bradford Hill criteria (BH criteria)** or **Hill's criteria for causation**: nine principles for establishing evidence of a causal relationship between two phenomena such as exposure to an agent (presumed cause) and disease (observed effect). Origin: Public health / epidemiology. Variations used also in toxicology and other areas.



Cyber incident leading to interruption and/or deterioration of healthcare services

Delayed health impacts



Conclusion

The JRC framework for CIH characterisation

1. **based on a consistent terminology (JRC ontologies)**
2. **provides a comprehensive characterisation approach of CIH**, allowing more detailed understanding of potential consequences on **healthcare delivery** and **patient safety**
3. **supports meaningful reporting and data exchange** based on a
 - **common set of attributes**
 - **analysis tools**
4. **allows more targeted mitigation measures**



Thank you!

This presentation has been prepared for internal purposes. The information and views expressed in it do not necessarily reflect an official position of the European Commission or of the European Union.

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](#) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

claudius.griesinger@ec.europa.eu

vittorio.reina@ec.europa.eu



Assessment of delayed health impacts

Spatio-temporal relationship: A spatio-temporal relationship between health impacts B in patients and a cyber incident A. The patients were interacting with a healthcare setting (spatiality) at a period (temporality) during which the setting was experiencing a cyber-attack.

Strength of association: It captures the observable and/or measurable strength of the suspected association between a phenomenon B and an antecedent event A: a strong association may support a possible mono-causal link while a weaker association may support a multicausal.

Scientific / clinical plausibility: It addresses the degree of alignment of a possible causal relationship between A and B with existing available scientific and/or clinical knowledge.

Consistency: is the suspected association of health impact B and cyber incident A consistent with observations from other healthcare settings, regions or countries that described a relationship between sufficiently similar incidents A* and similar health effects B*.

Analogy: Is the suspected association of health impact B and cyber incident A supported by analogous observations from other circumstances A' that led to healthcare service interruptions or deteriorations (such as staff strikes, IT outage, power cuts, lack of care delivery due to a public health emergency) and which led to health impacts B'?

Assessment of delayed health impacts

