EU legislative framework + Action Plan on cybersecurity of hospitals and healthcare providers

AIM – EHFCN Joint Event on Healthcare Cybersecurity

12 December 2024

Juuso JÄRVINIEMI, Policy Officer, Cybersecurity & Digital Privacy Policy

Status of the legal framework

European Commission

EU Cybersecurity Strategic Approach

PREVENT

- Network and Information Security (NIS2)
- Cybersecurity Act (certification)
- EU toolbox for 5G security
- Risk Assessments, de-risking of supply chains (5G toolbox, ...)
- Emerging tech / threats esp. post-quantum cryptography and AI
- Cyber Resilience Act (CRA)
- Cyber Solidarity Act (CySol)

DETECT

- European Cybersecurity Alert System made up of Cyber Hubs – (Cyber Solidarity Act)
- Information sharing via the CSIRTs network
- COM Cyber Situation Centre (with ENISA, CERT-EU)

RESPOND

- Cyber crisis response
  - EU-CyCLONe
  - EUIBAs (Task Force)
- Cybersecurity Emergency Mechanisms (Cyber Solidarity Act)
  - EU Cybersecurity Reserve
  - Mutual Assistance

DETER

- Cyber Defence Policy (coordination mechanisms between EU and MS, investment in R&D, EU-NATO cooperation, civil-military cooperation, etc.)
- Sanctions and wider Cyber Diplomacy Toolbox

INVEST IN CYBER CAPABILITIES (EU + Member States + industry)

- Digital Europe Programme
- Horizon Europe
- Recovery & Resilience Facility (RRF)
- European Cybersecurity Competence Centre
- ENISA
- Cybersecurity Skills and Awareness (Cyber Skills Academy)

International cooperation (cyber dialogues, digital dialogues and institutional cooperation)

NIS2 Directive

Transposition deadline – 17 October 2024

National measures shall be applied from 18 October 2024

Sectors of high criticality

- Healthcare providers
- EU reference laboratories
- R&D of medicinal products
- Manufacture of basic pharmaceutical products
- Manufacture of medical devices critical during public health emergency

Other critical sectors

- Manufacture of medical devices & in-vitro diagnostic medical devices

Cyber Resilience Act & Cyber Solidarity Act

Cyber Resilience Act → Entered into force 10 December → 36-month transition period

Not applicable to medical devices or in-vitro diagnostic medical devices for human use & accessories

SaaS (e.g. EHR): Connection to NIS2 implementing act (2024/2690) → security in systems acquisition, development & maintenance

Cyber Solidarity Act → To be adopted soon

Action Plan on the cybersecurity of hospitals & healthcare providers

Key cybersecurity challenges in healthcare

Types of threats[1]

- Ransomware attacks
- Data breaches
- Denial of service attacks
- Social engineering threats
- Supply chain attacks

Growing amount, value and reliance on sensitive health data

Human skills, training, capacity related factors

Impacting factors

- Increasing digitalisation in healthcare
  - Use of electronic health records is growing in hospitals and physicians' offices across OECD countries: **70%** → **93%** from 2012 to 2021[2]
- Shortage of qualified cybersecurity staff
- Lack of security awareness and training
- Shortage in cybersecurity skills
- Low cybersecurity maturity
- Legacy systems
- Fragmentation

1 ENISA Threat Landscape Report 2024, ENISA Health Threat Landsacape 2023
2 OECD's Health at a Glance 2023 report

Key aims of the Action Plan

Protect health systems against cyber & ransomware attacks

Threat detection

Preparedness

Crisis response