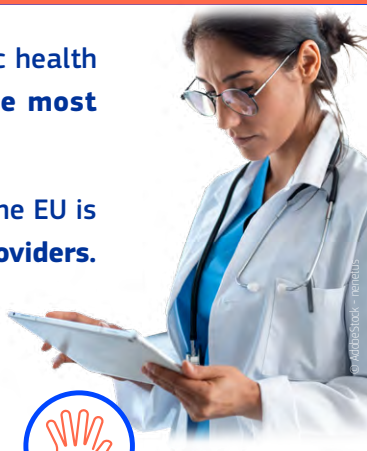
European Commission

Cybersecurity of hospitals and healthcare providers

January 2025

#DigitalEU #HealthUnion



Digitalisation of health services brings many benefits to patients, including electronic health records, telemedicine, and AI-driven diagnostics. However, **healthcare is one of the most targeted sectors by cyber and ransomware attacks.**

To better protect its healthcare systems and create a safer environment for patients, the EU is launching a **European action plan on the cybersecurity of hospitals and healthcare providers.**

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 KEY FIGURES AND CHALLENGES

309

cybersecurity incidents are reported by Member States in 2023 in the health sector.

Source: Annual report NIS directive Incidents 2023

54%

of incidents were ransomware* in the health sector (2021-2023).

Source: ENISA Threat Landscape: Health Sector (July 2023)

81%

of companies view difficulties in hiring cybersecurity staff as a risk for cyberattacks.

Source: 2024 Eurobarometer on Cyberskills

66%

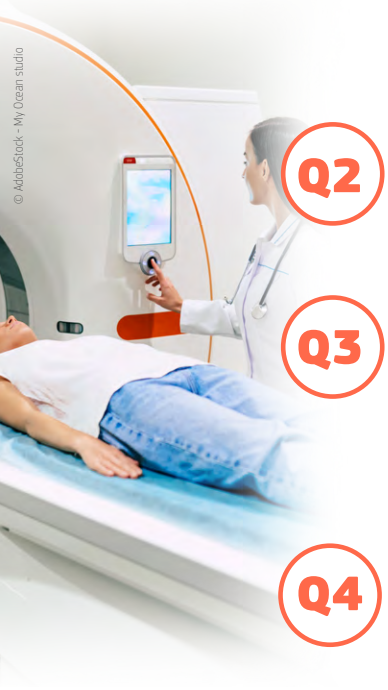
of cybersecurity roles are filled by employees transitioning from non-cybersecurity positions.

Source: 2024 Eurobarometer on Cyberskills

* A ransomware incident is a type of cyberattack where unauthorised parties gain access to and encrypt sensitive data rendering it inaccessible, and demand payment in exchange for the decryption key.

MAIN ACTIONS

ENISA, the EU agency for cybersecurity, will support hospitals and healthcare providers through its new **European Cybersecurity Support Centre**.



2025

Q1

- Launch **stakeholder consultations**.
- Set up a joint **Health Cybersecurity Advisory Board**.
- Explore options to give support to health sector for **preparedness testing**.
- Develop a **regulatory mapping tool** to help minimise the administrative burden.

Q2

- Begin work to establish a **European Cybersecurity Support Centre** for hospitals and healthcare providers.
- Call on cybersecurity stakeholders to **pledge actions** to address the challenges.

Q3

- Develop **guidance on most critical cybersecurity practices**.
- Create a framework for cybersecurity maturity assessments.
- Set up new procurement guidelines for cybersecurity in healthcare.
- Offer **guidance to help healthcare providers avoid paying ransoms**.

Q4

- Include a **Rapid Response Service** for the healthcare sector in the EU Cybersecurity Reserve.
- Build up a **European known exploited vulnerabilities** catalogue for medical devices, EHRs and ICT providers.
- **Identify key ransomware strains targeting healthcare**.
- Adopt **recommendations to further refine the Action Plan**.
- Launch pilot projects to develop **best practices for cyber hygiene** and security risk assessment.

2025-2026

- Carry out an **annual Health Cyber Maturity Assessment**.
- Create Cybersecurity **Voucher programmes** providing financial assistance to implement cybersecurity measures.
- Boost international cooperation against ransomware actors, notably through the **International Counter Ransomware Initiative** and the **G7** Cybersecurity Working Group.

2026

- Design **training modules and courses** for healthcare professionals.
- Create an **EU-wide early warning subscription service** and a **ransomware recovery subscription service for the health sector**.

Luxembourg: Publications Office of the European Union, 2025

Print ISBN 978-92-68-23802-8 doi:10.2759/5518411 KK-01-25-020-EN-C

PDF ISBN 978-92-68-23801-1 doi:10.2759/5713254 KK-01-25-020-EN-N