



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA's efforts in health cybersecurity

Maria Papaphilippou
Flora Tzagaraki

Resilience of Critical Sectors Unit

1. What is the Health Action Plan (HAP)
2. Timeline for implementation

1

What is the Health Action Plan (HAP)

EU action plan for the cybersecurity of hospitals and healthcare providers

- Published on 15.1.2025

- Objective 

Enhance cybersecurity resilience in hospitals and healthcare providers across the EU

- Strategic Pillars

 Prevent incidents	Risk management, training, preparedness
 Detect threats	Early warning system, detection tools
 Respond and recover	Incident response teams, EU reserve
 Deter malicious actors	Legal tools & cyber diplomacy



Brussels, 15.1.2025
COM(2025) 10 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL
COMMITTEE AND THE COMMITTEE OF THE REGIONS

European action plan on the cybersecurity of hospitals and healthcare providers

One holistic plan to support the health sector

Designed to reduce overlaps and increase complementarity

Support Mechanism (ENISA and EC for the MS)

- Service catalogue
- MS authorities to assess the services required (similar to Support Action model)
- Services delivered to health entities

Ongoing (next slides)

Funding to strengthen cybersecurity (ECCC and EC)

- DEP-8 call dedicated action to reinforcing hospitals and healthcare providers - 30M €
- Projects to support the services development (with the option to be included under the Support Mechanism)

Proposals evaluated

Vouchers program for hospitals and healthcare providers (EC)

- Regional funds to be distributed to entities
- Coordination and distribution by DG REGIO
- Monitoring by DG CNECT

Under preparation

Preparedness testing under CSoA (EC and ECCC) *

- DEP-9 call pilots on Health and Telecoms - 10M €

Call closed March 2026

* Additional services related to incident prevention and response also available via conversion of IR retainers (Cybersecurity Reserve)

2

Timeline for implementation



Support Mechanism

Timeline for implementation



**HEALTH
ACTION
PLAN**

December 2025

Signed the
Contribution
Agreement with the
Commission
6M € for three
years

March 2026

Launch of the
implementation period

- Service catalogue
- Coordination of the
Support Mechanism
- Align with ECCC
regarding DEP calls
- **HPoC model for
delivery**

Year 2

Regular progress
reporting to the
Commission

- Activities carried out
during the period
- Results

Year 3

Final report to
the Commission

2029 onwards

Assessment of
sustainability of
the action

The role of the Health Points of Contact (HPoC)

...is key!

- **Support** the **distribution at national level** of EU guidance, best practices, recommendations and tools developed under the Health Action Plan.
- Foster **cooperation, coordination and consistency** between the national **health** and **cybersecurity** authorities and any other relevant regulatory and supervisory bodies.
- **Support monitoring** of the **implementation** of the Health Action Plan at national level.
- **They are the primary coordination and communication interface** between the MS and EU-level bodies for all matters related to the implementation of the Health Action Plan.

1st HPoC meeting : July 2026

- EU survey on the theme of awareness campaigns
- Procedure



**HEALTH
ACTION
PLAN**

...HPoCs empower service delivery

Three-year forecast: YEAR 1 (1/4)

March 2026 - February 2027

Completed

- Cyber hygiene for health*
- Procurement guidelines for the cybersecurity of hospitals and healthcare providers*

- <https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector>
- [Procurement guidelines for the cybersecurity of hospitals and healthcare providers | ENISA](#)

In progress

- Interaction with Member States and relevant sector stakeholders
- Health Points of Contact (HPoC) at national level designated
- Support of the EH-ISAC and interaction with the Health Cybersecurity Advisory Board
- 3/5 CA FGIV recruited
- Risk assessment on medical devices (2026 Q4)
- Regulatory mapping tool (2026 Q4)
- Maturity assessment tool for entities (2026 Q4)
- 2 awareness campaigns: 1st based on hygiene* (2026 Q4)

Three-year forecast: YEAR 1 (2/4)

Regulatory mapping tool (2026 Q4)

An efficient tool for regulatory compliance

Complete a quick questionnaire and receive a personalized list of applicable regulations. Bridge the gap between law and practice by mapping regulatory requirements to recognized technical standards.

Open questionnaire →



Identify applicable regulations

Determine which EU cybersecurity legislations apply to your organization based on your specific entity type, size, and country of operation



Compare with technical standards

Compare your legal obligations side-by-side with industry-leading standards on information security.



Save or export results

Export a customized mapping of regulatory articles and technical controls in XLSX or CSV formats to support your internal compliance planning and audits.



Restart R

- Web-based tool
- Structured questionnaire
- Dynamic presentation of applicable cybersecurity requirements

Three-year forecast: YEAR 1 (3/4)

Maturity assessment tool for entities (2026 Q4)

- Web-based tool
- Actionable insights into vulnerabilities
- Demonstrate cybersecurity readiness to patients and stakeholders



This free self-assessment tool helps small and medium-sized organizations in the health sector understand and improve their cybersecurity posture.

One-off assessment



Complete the assessment without signing in. Suitable for a one-off time use. Your data will be processed according to the one-off retention policy.

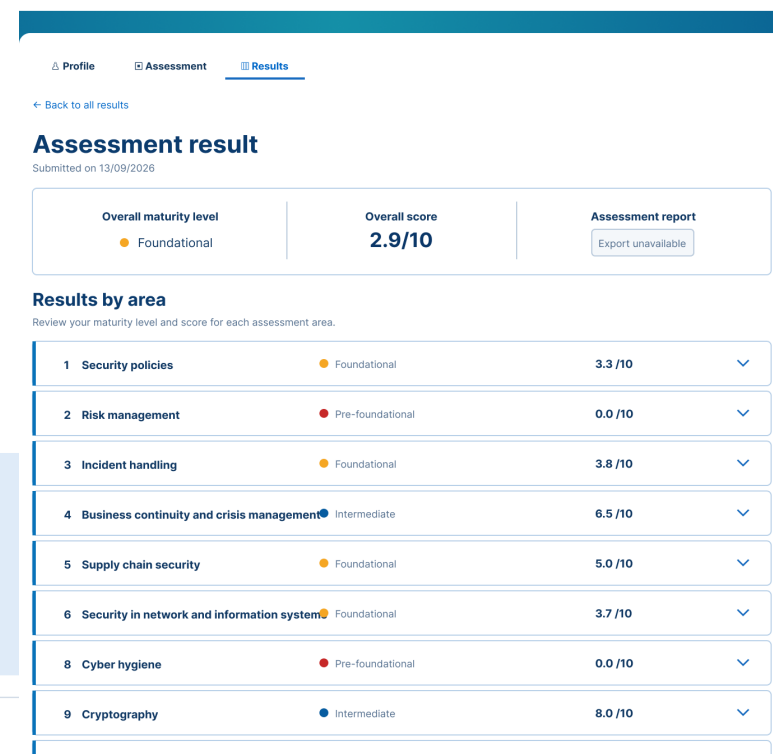
[START ONE-OFF ASSESSMENT →](#)



Track progress over time

Sign in with EU Login to save assessments, revisit previous results, and monitor progress over time.

[SIGN IN WITH EU LOGIN →](#)



The screenshot shows the 'Results' tab of the assessment tool. It displays the overall maturity level as 'Foundational' with a score of 2.9/10. Below this, a table lists results by area for nine categories: Security policies (3.3/10, Foundational), Risk management (0.0/10, Pre-foundational), Incident handling (3.8/10, Foundational), Business continuity and crisis management (6.5/10, Intermediate), Supply chain security (5.0/10, Foundational), Security in network and information system (3.7/10, Foundational), Cyber hygiene (0.0/10, Pre-foundational), Cryptography (8.0/10, Intermediate), and an additional category (0.0/10, Pre-foundational).

Profile	Assessment	Results
← Back to all results		
Assessment result		
Submitted on 13/09/2026		
Overall maturity level ● Foundational	Overall score 2.9/10	Assessment report Export unavailable
Results by area		
Review your maturity level and score for each assessment area.		
1 Security policies	● Foundational	3.3 /10
2 Risk management	● Pre-foundational	0.0 /10
3 Incident handling	● Foundational	3.8 /10
4 Business continuity and crisis management	● Intermediate	6.5 /10
5 Supply chain security	● Foundational	5.0 /10
6 Security in network and information system	● Foundational	3.7 /10
8 Cyber hygiene	● Pre-foundational	0.0 /10
9 Cryptography	● Intermediate	8.0 /10
...	...	...

Three-year forecast: YEAR 1 (4/4)

Q1 2027

Underway...

- Incident response playbooks tailored for health, with CSIRTs Network
- Customisation and development of content/scenarios for health national or regional exercises
- Europol's no more ransom project's expansion for health
- EU-wide early warning system
- Known Exploited Vulnerabilities (KEV) catalogue for health
- Training modules for healthcare professionals

Three-year forecast: YEAR 2

March 2027 - February 2028

Y1 services continued + New:

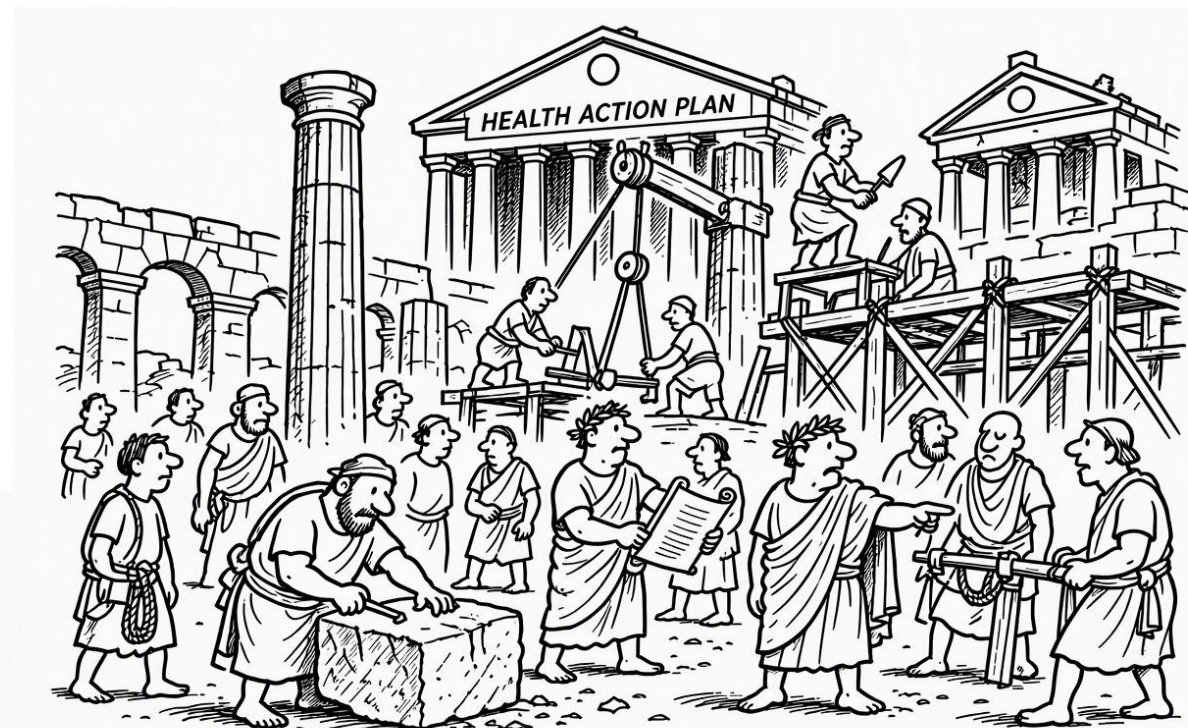
- Guidance for entities to avoid paying ransom
- Annual cybersecurity maturity assessments at EU level
- 2 more awareness campaigns
- National or regional cyber exercises for health, in hot-line mode, to test the playbooks and strengthen incident response protocols

Three-year forecast: YEAR 3

March 2028 - February 2029

Y1+Y2 services continued + New:

- Repository of tools at national level
- 2 more awareness campaigns (6 in total)



Rome wasn't built in a day...but we are getting there!



HEALTH ACTION PLAN

Thank you for your attention



+30 28 14 40 9711



info@enisa.europa.eu



enisa.europa.eu

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium