

(English version)

**Question for written answer E-002715/25
to the Commission
Ioan-Rareş Bogdan (PPE)
(2 July 2025)**

Subject: Cybersecurity in the medical sector

The growing digitalisation of healthcare services, the increased interconnectivity of medical devices and the pressure to provide rapid, technology-driven care have exposed weaknesses that have potential cross-border implications within the EU.

Recent years have seen an increase in cyberattacks targeting hospitals and healthcare providers across the European Union. Healthcare systems, often operating with legacy IT infrastructure and limited cybersecurity resources, have become particularly vulnerable targets.

1. What specific steps could the Commission take to help ensure that hospitals and healthcare providers across the EU have access to the necessary tools, expertise and financial resources to strengthen their cybersecurity, particularly in the face of growing threats such as ransomware attacks and disruptions to critical medical services?
2. Does it plan to propose a dedicated action plan or specific funding line to address the cybersecurity gaps in the healthcare sector?
3. How is the Commission facilitating cross-border cooperation and the exchange of best practices among Member States to ensure that cybersecurity incidents affecting healthcare infrastructure are effectively prevented, reported and mitigated at the EU level?

Submitted: 2.7.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(8 September 2025)**

In line with its Political Guidelines ⁽¹⁾, the Commission adopted in January 2025, a European action plan on the cybersecurity of hospitals and healthcare providers ⁽²⁾.

The action plan sets out a range of measures and practical tools, strengthening the security of our healthcare systems. For example, the European Union Agency for Cybersecurity (ENISA) should develop a comprehensive service catalogue for the needs of hospitals and healthcare providers, outlining available services for preparedness, prevention, detection and response against cybersecurity threats, including ransomware attacks and disruptions of critical medical services.

It also sets out measures for financial support to hospitals and healthcare providers. The European Cybersecurity Competence Centre has opened a call for proposals for a dedicated action to reinforce hospitals and healthcare providers ⁽³⁾.

Member States are encouraged to take measures like Cybersecurity Vouchers for micro, small and medium-sized hospitals and healthcare providers, which could draw from EU funds.

For future actions, the Commission proposal for the European Competitiveness Fund ⁽⁴⁾ includes a focus on a high level of cybersecurity and on the digital transformation of healthcare.

Health is also a critical sector under Directive 2022/2555 ⁽⁵⁾, which involves cross-border cooperation between Member States in various forums ⁽⁶⁾.

The action plan calls on ENISA, working with national authorities and drawing from the experiences of hospitals and healthcare providers, to develop a repository of available instruments at European, national and regional levels.

The Commission is committed to these efforts and intends to come forward with recommendations to further refine the action plan.

⁽¹⁾ Political Guidelines for the Next European Commission 2024-2029 https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

⁽²⁾ COM(2025) 10 final.

⁽³⁾ DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH.

⁽⁴⁾ Proposal for a regulation of the European Parliament and of the Council on establishing the European Competitiveness Fund. COM(2025) 555 final.

⁽⁵⁾ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

⁽⁶⁾ For example through the Network and Information Systems Cooperation Group. See <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>.