

**Question for written answer E-002715/2025/rev.1
to the Commission**
Rule 144
Ioan-Rareş Bogdan (PPE)

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