Council of the European Union

Brussels, 26 May 2025
(OR. en)

9351/25

TELECOM 161
CYBER 146

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	AOB for the meeting of the Transport, Telecommunications ans Energy Council on 6 June 2025 : European Action Plan on the cybersecurity of hospitals nand healthcare providers - Information from the Commission

European Action Plan on the cybersecurity of hospitals and healthcare providers

Secure and resilient healthcare systems are a cornerstone of the EU's social model. Cyberattacks against the healthcare sector cause direct harm to people, putting lives at risk. The cyber maturity of the health sector is in the lower end of the spectrum, yet the sector is a prime target for vicious ransomware attacks, seeking to disrupt operations and steal sensitive patient data.

The Political Guidelines for the 2024–2029 Commission therefore highlight the need to protect the security of European health systems against cyber and ransomware attacks. Consequently, the Political Guidelines committed to proposing a European action plan on the cybersecurity of hospitals and healthcare providers in the first 100 days of the new Commission mandate.

On 15 January, the Commission adopted a Communication[1] on the Action Plan. The Communication sets out actions for prevention, detection, response, recovery and deterrence against cyber threats to the healthcare sector. The Action Plan builds on the EU's legislative framework for cybersecurity, including the NIS2 Directive[2], the Cyber Solidarity Act[3] and the European Health Data Space Regulation[4], in order to ensure practical support for hospitals and healthcare providers.

[1] COM(2025)10 final.
[2] Directive (EU) 2022/2555.
[3] Regulation (EU) 2025/38.
[4] Regulation (EU) 2025/327.

Instead of adding new regulatory obligations for the sector, the Action Plan provides for developing specific guidance documents and resources that support healthcare organisations in their daily work. For example, the Action Plan envisages the development of guidance on the most critical cybersecurity practices to be taken by healthcare organisations, cybersecurity training resources for healthcare professionals, and playbooks to guide healthcare organisations in responding to cybersecurity incidents.

Moreover, the Action Plan will bring together professionals from the cybersecurity and healthcare sectors in networks, including a dedicated Health Cybersecurity Advisory Board[5] and the European Health CISOs[6] Network, to foster exchanges and sharing of best practices. The Action Plan also sets out measures to support the European Health ISAC[7], which serves as a platform for sharing threat intelligence among players in the sector.

The Action Plan also ensures some EU financial support for projects dedicated to cybersecurity in the sector, to be funded under the Digital Europe Programme. Furthermore, the Commission encourages the effective rollout of Cybersecurity Vouchers, funded for example through the European Regional Development Fund, to support the introduction of specific cybersecurity measures by hospitals and healthcare providers.

The Action Plan also addresses cybersecurity in healthcare supply chains, including connected medical devices. This includes carrying out a security risk assessment for medical devices, addressing both technical and strategic risks, and proposing mitigating measures.

The European Union Agency for Cybersecurity (ENISA) will play an important role in the implementation of the Action Plan, through a Support Centre for hospitals and healthcare providers that will operate within ENISA's structures. The 2025–2027 Digital Europe Work Programme allocates EUR 6 million for the Support Centre, in view of ensuring its appropriate resourcing.

Close cooperation with Member States is crucial for the successful implementation of the Action Plan. The Action Plan encourages Member States to take dedicated actions for cybersecurity in the healthcare sector, including by drawing up national action plans and non-binding funding targets.

In Q4 2025, the Commission intends to come forward with recommendations to further refine the Action Plan. In view of the upcoming recommendations, the Commission is engaging in detailed exchanges with Member States' health and cybersecurity authorities. The Commission is running a comprehensive consultation until 30 June, the results of which will feed into the further recommendations.

The Commission is committed to ensuring continued exchange with the Member States to ensure successful implementation of the Action Plan.

---

5 The group was created in April 2025. The Commission is currently reviewing applications for membership of the group.

6 Chief Information Security Officers

7 Information Sharing & Analysis Centre