Stockholm Region Association for European Affairs position on the

European action plan on the cybersecurity of hospitals and healthcare providers

Introduction

The healthcare sector is undergoing a profound digital transition that is reshaping both working methods and encounters with healthcare providers. Digital services, medical technologies and new organisational practices create vast opportunities, while dependence on digital infrastructure is growing rapidly. With increased digitalisation, however, come heightened risks. The European healthcare sector is a critical societal function that is exposed to cyber threats largely due to outdated IT infrastructure, fragmented practices and uneven implementation of security measures. Diverging conditions among Member States and health care providers further complicate coherent cybersecurity efforts.

In this context, the Commission's proposed action plan for cybersecurity in hospitals and healthcare providers plays a pivotal role. The action plan contains several valuable measures and has the potential to become a key instrument for driving real improvements in healthcare cybersecurity across Europe. It could set a common direction and foster coordinated actions that enhance resilience against diverse cyber threats. To succeed, the action plan must be concrete, goal-oriented and ambitious – with clear links to existing legislation and initiatives, while ensuring effective implementation capacity across providers regardless of national contexts. At the same time, it is important that cybersecurity measures do not unintentionally hinder information-sharing and collaboration within the already fragmented systems of healthcare. Against this background, the Stockholm Region Association for European Affairs wishes to contribute concrete recommendations to strengthen the practical impact of the action plan.

Stockholm Region Association for European Affairs position Summarised in Three Recommendations

1. *Build on existing initiatives, legislation and cooperation structures to create tangible added value and avoid unnecessary administrative burdens*

2. *Accelerate the action plan's implementation capacity through clear allocation of responsibilities and measurable objectives*

3. *The action plan should strengthen cybersecurity maturity among healthcare providers by enhancing internal capacity, in parallel with measures against external threats*

Stockholm Region Association for European Affairs consists of three main members: the City of Stockholm, Region Stockholm and Storsthlm. Other members in the association are Region Uppsala, Region Västmanland, Region Sörmland, Region Gotland, and Mälardalsrådet – the Council of the Stockholm-Mälar Region. The association aims to promote the members' common political interests through collaboration on issues connected to the region's relationship with the EU. Together the members own the Stockholm Region EU Office, their joint representative office in Brussels

Recommendations

Develop existing initiatives to strengthen cybersecurity in healthcare

- The Stockholm Region Association for European Affairs welcomes the emphasis on trust-based cooperation. The action plan should primarily aim to reinforce the systematic cybersecurity capacity of European healthcare providers and support prevention and incident management.

- While enhanced EU-level cooperation in cybersecurity is welcomed, the focus should be on strengthening and coordinating existing structures – such as EU-CyCLONe, the CSIRT network, the NIS Cooperation Group, the Health Workstream and the ECCC – rather than establishing new initiatives that risk duplication and blurred lines of responsibility.

- The implementation of existing and forthcoming legislative acts relevant to healthcare cybersecurity must be the action plan's core focus. Legislations such as the General Data Protection Regulation (GDPR), the Artificial Intelligence Act, and the NIS2 Directive already impose significant requirements. The action plan should act as a catalyst for their implementation, including concrete actions that operationalise their ambitions both in the short and long term. This would strengthen the plan's legitimacy and strategic value.

- The action plan should also leverage initiatives such as the Union of Skills, ESF+ and other funding instruments to mobilise competence development in healthcare cybersecurity. These can channel resources towards training, continuous professional development and recruitment of qualified cybersecurity professionals for hospitals and health care providers.

For the action plan to have impact, it must be supported by concrete and measurable objectives and be allocated clear budgetary frameworks

- The Association stresses that implementation would be strengthened if the plan were linked to clear, measurable objectives, with each measure assigned to a responsible actor. Areas identified for improvement should be allocated transparent budgetary resources. This would facilitate evaluation of effectiveness and long-term impact. The Swedish National Cybersecurity Strategy[1] offers a good example, with clearly defined responsibilities, objectives and scope set out in a structured and transparent way.

- The action plan should also signal a higher level of ambition in driving harmonisation among Member States, raising Europe's digital environments to a new common level. This is essential to secure both flexibility and digital sovereignty in digital services and healthcare IT infrastructures.

[1] En ny era av cybersäkerhet. Nationell strategi för cybersäkerhet 2025–2029. Skr. 2024/25:121. https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-for-cybersakerhet-2025-2029/

- The action plan's practical impact would be greater if it included specific measures to stimulate the growth of European digital services and protective solutions through public–private cooperation, both in times of peace and in crises. As actors in these sectors operate under diverse legal, organisational and technical conditions, measures and support must be adapted accordingly.

Concentrate the scope of the action plan to promote cybersecurity maturity within the EU healthcare sector

- Beyond external threats and cyberattacks, the Association also highlights the importance of addressing broader aspects that shape cybersecurity, including internal organisational conditions such as modernisation and standardisation of IT environments, implementation of protective measures, access to qualified staff, and continuity planning. These are foundational to strengthening cybersecurity, adapting to external changes and achieving a coordinated, sustainable level of protection across the EU healthcare sector.

- To ensure a consistent interpretation and application of the action plan, it is important that clear definitions of healthcare, healthcare providers, and health data are used. This will create the conditions for effective coordination, clear allocation of responsibilities, and legal certainty for the actors concerned such as healthcare providers, social services, and care providers at both national and European level.

- The action plan would benefit from a clear focus on activities that raise cybersecurity maturity. A harmonised level of cybersecurity maturity within the EU healthcare sector will also facilitate the implementation of other legislative acts in the field, such as the Regulation on the European Health Data Space (EHDS) and the GDPR, thereby ensuring the protection of patients' rights and freedoms. Another example is the review of organisations' internal digital capacity, for instance ensuring that electronic health record systems and other digital tools in one Member State can communicate with corresponding systems in other EU countries. Other important areas include preparing for full interoperability in line with EU standards regarding cross-border data sharing. An action plan that explicitly prioritises accelerating cybersecurity maturity among healthcare actors within the EU will benefit this development.

The action plan should establish a systematic framework for exercises and testing across the healthcare system

- The Association stresses the importance of regular cyber exercises and threat-driven testing at local, national, multinational and EU level to strengthen cross-border cooperation and common preparedness in healthcare. The action plan should actively promote and support such exercises and ensure that they are designed to not only enhance cooperation between actors but also enable systematic identification of vulnerabilities that could be exploited by threat actors.