June 2025

HOPE Position on the European Action Plan on the cybersecurity of hospitals and healthcare providers

HOPE greatly welcomes the release of the European Commission's Action Plan on the cybersecurity of hospitals and healthcare providers[1], the prioritisation of which demonstrates political commitment to this issue at a time of great uncertainty. The Communication sends an unmistakable signal to reinforce and harmonise the European planning and coordination effort in the sector and responds to recurring HOPE calls for increased action to better protect the healthcare ecosystem.[2]

All things considered, the Action Plan is comprehensive – covering the entire cyber threat cycle (prevention, detection, response, recovery, deterrence) –, addresses key healthcare and cybersecurity actors, and emphasises the urgent need for improved reporting as well as guidelines for easy-to-implement good practices and protocols. The importance placed on awareness-raising and training across different healthcare settings in Europe is also appreciated.

There are nonetheless a few points where HOPE feels clarification is required, the proposed actions could be enhanced or modified, or that risk compromising its effective realisation. HOPE calls on the Commission to swiftly refine the Action Plan based on the inputs received from the public consultation, and to ensure its solid and committed implementation.

Funding

A key flaw of the Action Plan is the lack of additional European funding attached to it, as has been pointed out by Members of the European Parliament upon its release.

While HOPE recognises that the action plan represents first and foremost a framework for bringing together all relevant instruments, good practices and stakeholders to pool resources and equip all relevant actors with the information, knowledge and tools to anticipate, thwart and react to cyber-attacks, the strategic targeting of critical infrastructures justifies dedicated financing of actions concomitant to the menace. The impacts of large-scale cyber- or hybrid attacks could be a lot more far-reaching than harming hospitals and their patients: they can impair entire states and societies by incapacitating indispensable services while simultaneously seizing highly sensitive data. Increased reliance on data flows in a digital world means that defence, cybersecurity and economic policies are closely intertwined; this link is recognised, inter alia, in the White Paper for European Defence – Readiness 2030[3] (part of a broader defence policy package including loan facilities), the International

[1] COM(2025) 10 final
[2] HOPE Position Paper on the EU Cybersecurity Framework (2023), https://hope.be/wp-content/uploads/2023/12/HOPE_Position_EU_Cybersecurity_FW_final_Dec2023-1.pdf
[3] https://defence-industry-space.ec.europa.eu/eu-defence-industry/introducing-white-paper-european-defence-and-rearm-europe-plan-readiness-2030_en

Digital Strategy for Europe[4], and the European Internal Security Strategy (ProtectEU)[5]. Healthcare being a major target for cyber-criminals, HOPE urges the Commission to link these policy agendas not only discursively, but also financially. This could open up avenues for additional funding to make certain that *all hospitals and healthcare providers across Europe* are able to access and deploy cybersecurity resources commensurate with the threat.

The need for appropriate financing becomes clear when looking at the French CaRE programme[6] referred to in the Action Plan, which gathers and mobilises national and regional healthcare cybersecurity stakeholders in a collaborative effort to execute a countrywide strategy and assign funding. Such a systemic endeavour is still far removed from the reality in many Member States, which exhibit lower levels of cybersecurity maturity and lack comparable cooperation mechanisms.

At institutional level, many hospitals and healthcare providers are using outdated systems that present safety issues due to their size and complexity. Simultaneously, the introduction of state-of-the-art EHR systems and artificial intelligence (AI) tools is accompanied by new threats requiring a parallel increase in vigilance, which also comes at a cost. Healthcare cybersecurity thus involves a permanent cycle of investing and learning that challenges sectoral capacities and modus operandi.

Although the funding already secured under the Action Plan for the establishment of ENISA's Cybersecurity Support Centre and its pilots (through the Digital Europe Programme) will help close important knowledge and procedural gaps, and the proposed voucher scheme (via the European Regional Development Fund) could be a windfall for numerous small healthcare providers, the question remains how robust and far-reaching multi-stakeholder actions can be achieved to protect health services and patients across the EU. While the NIS2 Directive is an important driver for increased cybersecurity investments by governments and at healthcare institutional level, HOPE cautions that, without additional earmarked EU funding, the attainment of tangible progress will be doubtful. The delays experienced in the national transposition of NIS2 and Critical Entities Resilience (CER) Directives are a salient reminder.

As the European Health Data Space (EHDS) connects healthcare stakeholders more intricately across institutional and geographic boundaries, HOPE calls on the Commission to provide sustained cybersecurity financing for all hospitals and healthcare providers. It is essential to avoid further digital fragmentation and 'cybersecurity deserts'. All Member States must possess sufficient resources to implement the proposed actions, which entails massive investments required for updating technologies, training millions of professionals, and developing strategies for individual institutions aligned with national action plans expressing domestic priorities, including law enforcement. The regions, too, must be able to access implementation funding, which is not always straightforward.

[4] JOIN(2025) 140 final
[5] COM(2025) 148 final
[6] https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf

Cybersecurity Support Centre

HOPE feels that the services outlined in the Action Plan, to be provided by the future Cybersecurity Support Centre, are mostly suitable as they fill important gaps across the cyber-threat cycle. As a platform for information exchange, the Support Centre should streamline guidance in all areas to strengthen Member States' efforts, especially for implementing NIS2, without defining additional overlapping requirements.

Particularly valuable are the proposed stock-taking, advisory and educational materials (service catalogue on critical cybersecurity practices, promoting standards, regulatory mapping tool, known exploited vulnerabilities catalogue, new procurement guidelines, healthcare-specific maturity assessment framework), the EU-wide subscription services (early warning, ransomware recovery), the development of incident response playbooks and coordination of national exercises, as well as providing assistance to Member States in developing national action plans.

However, a few tasks currently assigned to the Support Centre appear to impede rather than foster synergies with existing structures. This includes the coordination of the planned European Chief Information Security Officer (CISO) Network: a similar grouping has already been established by the European Health-ISAC (EH-ISAC) as a forum in which information and experiences are discussed openly yet confidentially, as is the case for national ISAC groups. Duplication or joint membership could decrease the participants' confidence. The EH-ISAC role could be expanded to receive early incident notifications from healthcare providers, shared anonymously within a trusted community to avoid concealment and reputational damage.

In addition, the coordination functions of the European Network of Cybersecurity Incident Response Teams (CSIRT), established to support the NIS Directive, as well as of the national CSIRTs, could be further strengthened. Given the importance of facilitating rapid and meaningful cross-border threat information exchanges between EU hospitals and ensuring that timely assistance can be provided to manage incidents, the CSIRTs are vital first points of contact. They should be well-connected and resourced to operate as efficiently as possible. It should be clarified how the EU Cybersecurity Reserve will be mobilised in case of national capacity restrictions and what the added value would be if CSIRTs were to double-function as National Cybersecurity Support Centres for hospitals and healthcare providers.

Therefore, HOPE considers it would be sensible for the Support Centre not to reinvent the wheel but rather to delegate certain sets of activities. Broadening the scope of EH-ISAC, for example, would be coherent with another role envisaged for it in the Action Plan, i.e. convening healthcare providers and manufacturers to discuss and develop a joint understanding of product security, assisted by the Support Centre.

At the same time, HOPE thinks there are other services the Support Centre would be well placed to carry out. One important task could be the conception and coordination of Europe-wide awareness-raising and cyber-hygiene campaigns targeting different hospital and healthcare staff, technology manufacturers and supply chain agents, and patients. Such campaigns should stress that cybersecurity is a shared responsibility of all stakeholders.

All European hospitals and healthcare providers should have tools at their disposal to proactively develop their own cybersecurity strategies. To this aim, they would benefit from real-world scenarios covering different types of threats and tailored support (overviews and in-depth advice on good practices) to prevent them. Tailoring toolkits with suitable cybersecurity practices to larger hospitals on the one hand and to small/medium sized clinics and healthcare providers on the other, reflecting their respective circumstances and needs based on size, IT capability, and degree of interconnectivity with external partners' networks, would be advantageous.

The Support Centre could also help make available digital tools to better control cyber threats and safeguard business continuity, similar to the cross-sectoral cybermeter used in Finland[7]; and to anticipate and simulate different threat scenarios and learn how to cope with them.

For individuals working in healthcare settings, the Support Centre could foster on- and offline resources including apps, flyers and flashcards, which could serve as 'memory aids' to spread good cyber-hygiene practices as part of routine care while mitigating stress in emergency situations by reminding all staff of the relevant processes in place.

More generally, the Support Centre's service repository should serve to strengthen the work at national and regional level by consolidating knowledge and incessantly promoting a few important basic cyber-hygiene practices including:

- Choosing and managing strong passwords and using multi-factor authentication;
- Handling e-mail and messaging tools properly to avert phishing attempts and related attacks;
- Restricting staff access to systems and networks they use, assigning privileges based on responsibility;
- Adopting two and multiple tier authorisation processes for certain network and cloud-based systems;
- Segmenting the network and allowing only approved equipment and software;
- Ensuring security updates are continuously installed, outdated software / hardware is upgraded or replaced in a timely manner;
- Disabling unused accounts, software and hardware;
- Ensuring regular back-ups and storing them securely;
- Prohibiting the use of removable media and connection of personal devices;
- Saving logs to examine the nature and evolution of incidents; and
- Enabling a return to paper-based operations when systems are down.

Training and education

Cybersecurity being an integral part of patient safety, the Commission should strive to ensure that healthcare professional education curricula include modules to build up digital literacy and an

[7] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

understanding of the security dangers inherent in data-powered tools, systems and AI models. In addition, continuous professional development and training should be available across the EU.

The challenge of educating so many people working within and around healthcare institutions necessitates a major effort that Cybersecurity Skills Academy resources and online courses alone cannot accomplish. NIS2 already obliges senior managers of essential and important entities to follow cybersecurity training and encourages similar training for other healthcare staff.

HOPE reminds the Commission that, given the current levels of staff shortages and resulting heavy workloads, high stress levels and operational pressures borne by healthcare professionals, they may not have the time to follow online courses unless provisions are made during work hours. It must be avoided that training becomes another burden or tick box exercise.

In addition, cybersecurity measures should match healthcare professionals' needs and competences, without disrupting workflows and patient care. It should be based on a thorough analysis of the ways in which hospitals are attacked and reflect specific circumstances rather than on assumptions. it is also vital to address the interplay between medical IT and operational technologies.

The proposed industry pledges for offering training or security services must not create advantages for a small group of select companies.

Regional and national actions

HOPE membership includes national and regional authorities in charge of organising the healthcare sector, in keeping with the different competences accorded to them.

In recent years, many regions have invested in digital health systems and processes, designed to meet specific needs and based on local priorities. This goes hand in hand with cybersecurity arrangements that function equally well under the aegis of the regions.

In some countries, regional authorities are operating in close proximity to local cybersecurity ecosystems: hospitals, other healthcare providers, professionals and patients, as well as technology companies including SMEs. In parallel, inter-regional projects and other regional cybersecurity initiatives can serve as testing grounds for identifying good practices and processing lessons learnt, potentially suitable for scaling up at national level. Nevertheless, the role of the regions in raising cybersecurity awareness and knowledge sharing is often overlooked. Regions are also catalysts for public-private partnerships, helping to ensure that identified concerns are addressed and tech providers do not operate in silos.

Therefore, HOPE thinks it is vital to integrate them into European and national actions and ensure their competences are respected in countries where they organise healthcare. In some Member States, a centralisation of cybersecurity powers could generate detrimental impacts by undermining networks formed at regional level.

Regarding national actions and roles, HOPE thinks that, in addition to devising national action plans, the functions proposed in the Action Plan (enabling joint procurement or pooling resources, setting benchmarks, monitoring funding targets) would be advantageous. They should complement existing

cybersecurity actions and investments initiated in the Member States. Where they exist, sector-specific national IT security standards and associated measures should be supported, which requires considerable financial resources.

The development of voluntary cybersecurity performance goals to create a baseline, foster leadership and support collaboration could also be fruitful. In the United States, the attainment of such goals is supported through publications and practical resources by the Cybersecurity and Infrastructure Security Agency (CISA) and its partner institutions. They include a comprehensive guide containing mitigation strategies for the areas of asset management and security; identity management and device security; vulnerability, patch and configuration management; and guidance on purchasing secure-by-design products.[8]

While sharing certain threat intelligence across Europe via the Support Centre – such as cyber incident notifications received anonymously by CSIRTs - is beneficial, other information, such as voluntary reporting of ransomware payments made or intended by healthcare providers subject to the NIS2 Directive, should stay at national level to protect the entities involved. HOPE points out that reliance on voluntary information – since NIS2 does not currently include such a requirement - risks painting a flawed picture.

It would be beneficial to have more transparency regarding the full costs incurred by different types of healthcare cyber-attacks across Europe, but again this information should be compiled and tracked domestically and shared internationally without damaging the reputation of affected entities.

Health Cybersecurity Advisory Board

HOPE agrees that fruitful public-private cooperation between healthcare and industry representatives is fundamental for the Action Plan's success. Hospitals and healthcare providers benefit greatly from the technical knowledge of cybersecurity companies and other specialised entities, and vice versa the latter need to be aware of everyday difficulties or flaws. This cooperation should be fostered by the Health Cybersecurity Advisory Board to develop a European approach to cybersecurity aligned with the people-centred, inclusive, rights-based vision that underwrites EU digital health policies.

It will be important to safeguard that providing quality care, and protecting patients' privacy and personal data, supersedes commercial interests. It would thus be advantageous to ensure close interactions with the networks and entities supporting the Action Plan's implementation (European CISO Network, CSIRTs, EH-ISAC, etc.) to ensure that real-world challenges are addressed.

The inclusion of HOPE in the Advisory Board as a representative of hospitals and healthcare providers is essential.

Other considerations

The Action Plan is but one element of a growing EU cybersecurity framework; by consolidating existing resources and offering new healthcare-specific services, it represents a milestone for the sector in conjunction with relevant pieces of EU legislation including NIS2, the Cyber Resilience and Cyber

[8] https://www.cisa.gov/resources-tools/resources/mitigation-guide-healthcare-and-public-health-hph-sector

Solidarity Acts and others. It should be closely linked to cross-sectoral initiatives including the upcoming EU Cybersecurity Strategy and the EU's defence package.

HOPE appreciates the Commission's understanding of healthcare being characterised by diverse actors and complex supply chains and recommends that a strong cybersecurity safety net should also encompass the evolving broader health ecosystem. This not only includes entities and professionals operating across different care settings (primary / secondary / tertiary care, residential and home care, community care, etc.), but also in wellness, fitness and health counselling.

Apart from encouraging manufacturers of medical devices to provide voluntary information about actively exploited vulnerabilities and incidents through the EU reporting platform under the Cyber Resilience Act, and asking cloud service providers to embed 'Security by Default and Design', the Action Plan does not propose any additional requirements for industry actors, which also include the pharmaceutical and biotechnology sectors. HOPE thinks this may be insufficient given the pace of innovation, polyvalent character of many digital solutions and uncertainty over compliance with cybersecurity legislation.

As the number of digital solutions in healthcare is continuously growing, and hospitals often outsource cybersecurity services to external providers, there is also a constant need for up-to-date standards and certification programmes.

The intention to encompass EU enlargement, neighbourhood and partner countries is far-sighted and necessary to ensure Europe's cybersecurity shield cannot be broken inadvertently. There is scope for increased collaboration with WHO/Europe in this area.[9]

HOPE also encourages the Commission to consider evolving and future technological trends (e.g., telemedicine, generative AI, personal AI tools used by staff for work purposes, wearables and fitness apps used by patients) and workplace practices (e.g., remote working across world regions, co-working spaces, job sharing, flexible leave policies, etc.) and their effects on managing cybersecurity.

Final remarks

Although non-binding, the European Action Plan on the cybersecurity of hospitals and healthcare providers represents an important umbrella which, by bringing together all available resources relevant to the sector, will contribute to the detection and closing of critical gaps and needs across the cyber security lifecycle. The support services and other actions proposed will help its beneficiaries to better integrate cybersecurity into their organisational structures, everyday operations, and to scale up actions.

Realising the Action Plan's ambition will require a strong multistakeholder effort, the success of which will partially depend on the availability of adequate implementation funding and inclusive governance.

[9] See WHO's 2025 guide on "Cybersecurity and privacy maturity assessment and strengthening for digital health information systems": https://www.who.int/europe/publications/i/item/WHO-EURO-2025-11827-51599-78854

****

HOPE, the European Hospital and Healthcare Federation, is a European non-profit organisation, created in 1966. HOPE represents national public and private hospitals associations and hospitals owners either federations of local and regional authorities or national health services. Today, HOPE is made up of 36 organisations coming from the 27 Member States of the European Union, as well as from the United Kingdom, Switzerland and Serbia as observer members. HOPE mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.