CCMI FACTSHEET:

CYBERSECURITY OF HOSPITALS AND HEALTHCARE PROVIDERS IN THE EU (CCMI/244)

The European Economic and Social Committee (EESC) adopted on 18 June 2025, an opinion strongly supporting the European Action Plan on the cybersecurity of hospitals and healthcare providers launched by the European Commission in January 2025. The EESC welcomes the level of ambition of this plan, which aims to continuously enhance the cyber resilience of healthcare entities against growing attacks (particularly ransomware). The healthcare sector, organised locally in Member States but increasingly interconnected (telemedicine, patient portals, connected medical devices, AI), is a prime target for malicious actors. The EESC insists on a rights-based approach, recognising cybersecurity as a fundamental right, alongside privacy, data protection, and physical safety. This opinion underlines the need to prioritize a sovereign European medical cloud and proposes concrete recommendations to address gaps, particularly in financing, technical, process, and educational measures, while highlighting risks related to cyber-physical systems (surgical robots, medical devices) and legacy systems.

KEY FACTS: THE URGENCY TO ACT

Cyber threats cause preventable disruptions with high human and economic costs.

Cyber threat in the healthcare sector: In 2020, ENISA reported a 47% increase in cyberattacks across the EU; in France, declared cases doubled in 2021.

Sector scale: Over 2.3 million hospital beds in the EU; more than 10 million health and social care personnel to be trained

Investment needs: Significant disparities between Member States (France: >€1. billion/year; EU extrapolation: minimum €7.5 billion/year). Recommendation: allocate around 10% of hospitals' IT budgets to cybersecurity

Incident costs: Up to €20 million per attack in France; multi-million euro remediation and recovery costs.

Current funding: €6 million for ENISA deemed insufficient. Underinvestment persists: many hospitals allocate <10% of IT budgets to cybersecurity, creating inequalities especially for small/rural providers

Context: Essential protection for citizens, the future European Health Data Space, and diverse entities (hospitals, emergency services, pharmaceuticals, biotechnology, research…).

RECOMMENDATIONS FROM EESC OPINION CCMI/244

The EESC proposes a systemic approach to strengthen cybersecurity.

1. Financial measures	✓ Regret over the lack of dedicated financial support, risking inequalities in protection. ✓ Encourage thematic concentration via cohesion funds; explore fast-tracked loans for ENISA and cyber tools dedicated to the health sector. ✓ Monitor territorial investments and map actual attack costs to better target funds (prevention, education, remediation). ✓ Consider health cybersecurity spending as defence expenditure or under the general escape clause of the Stability and Growth Pact. ✓ Strengthen the role of data protection authorities
2. Technical measures	✓ Promote basic digital hygiene (access control, disabling USB ports, antivirus, quarantining infected machines, network separation). ✓ Invest in digital twins for testing devices and systems. ✓ Support small structures without IT services (centralised secure servers via ENISA). ✓ Strengthen strategic capabilities (OT security, safety-security link, forensic readiness, AI). ✓ Pre-check all microprocessor-equipped devices before installation; limit external web access via disconnected PCs. ✓ Pay attention to legacy systems, IT/OT convergence, and cyber-physical systems
3. Process measures	✓ Conduct systematic tests (resistance, penetration) at all levels (device, system, operational). ✓ Develop and regularly audit business continuity plans, including degraded/manual mode and disconnected backups. ✓ Create a cybersecurity toolkit (resources, best practices, simulations). ✓ Enhance cooperation (CSIRTs, cross-border threat intelligence sharing; ethical hackers and NGOs). ✓ Manage internal threats via risk-based approach (access controls, balanced surveillance without intrusion). ✓ Integrate supplier cybersecurity certification, while avoiding additional costs for hospitals. ✓ Promote sovereign European medical clouds with multiple verifications.
4. Educational measures	✓ Targeted training (with social partners, micro-credentials under Union of Skills). ✓ Awareness campaigns of cyber literacy (digital hygiene, psychological risks of cyber stress). ✓ Knowledge transfer between entities; EU-funded campaigns. Include cybersecurity in health education; address multidisciplinary workforce gaps (cyber, AI, forensics, medical device security). ✓ Frequent simulations and attack exercises to test restoration plans. ✓ Social dialogue to manage institutional responses, privacy, and psychological stress.

ALIGNMENT WITH EU COMMISSION PRIORITIES FOR IMPLEMENTATION

Our recommendations amplify the Action Plan's four pillars (Prevent, Detect, Respond/Recover, Deter) while filling gaps in financing, ethics, and scope.

The EESC opinion fully aligns with the Commission's priorities: strengthening cyber resilience (European Declaration on Digital Rights and Principles for the Digital Decade, Cyber Resilience Act, EU AI Act, MDR), protecting the European Health Data Space, and initiatives such as the Union of Skills. It supports public-private cooperation while calling for caution (conflicts of interest, GDPR compliance, ethical clauses).

The EESC requests clarification of the scope of healthcare providers covered by the action plan (to confirm whether it exhaustively includes the broad health ecosystem and to account for indirect interactions with the wider ecosystem, including commercial well-being services) and a strengthened role for ENISA (technical assistance, e.g., providing software or secure servers; financial mapping of cybersecurity investments in MS).

The EESC complements the plan by emphasising a holistic vision (rights-based, cyber-physical, adequate financing) for an effective Preparedness Union, integrating social dialogue and partners for balanced and resilient implementation.