Technische Hochschule Brandenburg · Technische Hochschule Ingolstadt · Technische Hochschule Nürnberg Georg Simon Ohm

Technische Hochschule Brandenburg
Fachbereich Informatik und Medien
Prof. Dr. Michael Pilgermann
michael.pilgermann@th-brandenburg.de

Technische Hochschule Ingolstadt
Fakultät I
Prof. Patrizia Heinl
Patrizia.Heinl@thi.de

Technische Hochschule Nürnberg
Georg Simon Ohm
Prof. Dr. Andrius Patapovas
andrius.patapovas@th-nuernberg.de

European Commission
Directorate-General for Communications Networks, Content and Technology
European Commission
1049 Bruxelles/Brussel
Belgium
e-mail only: EC-HEALTHCARE-CYBERSECURITY@ec.europa.eu

Date
27.06.2025

Consultation on the European action plan on the cybersecurity of hospitals and healthcare providers

Dear Sir or Madam,

on 15th of January the European Commission published its action plan on the cybersecurity of hospitals and healthcare providers. With publication from 7th of April the European Commission launched a consultation on this action plan and invited experts and stakeholders to share their views. Please find our comments on the action plan below.

0) Introduction of signatory parties

We are professors at German universities who are dedicated to the topic of IT security in healthcare. In order to pool the few academic resources working on this topic, we jointly founded the working group 'Secure Digitalisation in Healthcare' within the German Informatics Society in 2024, thereby establishing a community of practitioners and academics to improve IT security in hospitals and healthcare in a structural and systematic manner.

1) Welcome the action plan

It is obvious (as the figures show) that IT security is a challenge in the operation of Critical Infrastructures, especially in hospitals. It must be recognised that IT security requires a certain level of capacity (both in terms of investment and, in particular, running costs (personnel)). It is now important to free the necessary resources for this, both in the coordinating activities at EU level (in particular the support center at ENISA) and at the operational level in hospitals.

2) Involve the policy level

Framework conditions are needed, particularly at the implementation level (hospitals as operators), in order to address the issue of IT security in a sustainable manner. There is sufficient awareness of the issue and a willingness to implement measures, but the financing arrangements in the federal system prevent operators from compensating for the corresponding costs. The action plan should include a review and optimisation of these framework conditions.

3) Integrate national preparatory work

The specific measures announced are welcome overall. However, it should be taken into account that preliminary work has already been carried out at national level and valuable experience has been gained. Using Germany as an example, it would be advisable to suggest that:

- the intensive and professional preliminary work carried out by B3S be taken up for the 'Guidance on most critical cybersecurity practices'; that this be translated and thus made more easily accessible to others;
- that the preparatory work on maturity levels in accordance with Section 8a BSIG for operators of critical infrastructures, and thus also hospitals, be taken up for the 'Cybersecurity maturity assessment'; and
- that the corresponding white paper from a working group of the UP KRITIS 'Supplier obligations' be taken into account for the 'Procurement Guidelines'.

4) Incorporate and consolidate research results

In recent years, EU research has addressed and significantly funded extremely useful topics related to IT security – examples include the AI4HealthSec, CyberSANE, Septon and SECANT projects. However, it turns out that these projects do not contribute substantially to improving IT security at the operational level in the operation of hospitals. The action plan should therefore be expanded to include this topic and promote greater practical relevance in research. In addition, despite the extensive resources made available, important foundations for further research are lacking, such as sector-specific data sets that could be used to test the effectiveness of innovations in a targeted manner.

5) Include cyber security for AI to support a safe and secure adoption of AI

As AI becomes increasingly integrated into clinical workflows and hospital infrastructure, it introduces new vulnerabilities and attack surfaces that must be addressed (Security for AI). Elements of third-party AI tools must be monitored as part of broader supply chain risk management efforts—particularly across the AI lifecycle, including data sources, training, testing, and inference procedures. Following the NIST AI Risk Management Framework, hospitals should map critical AI systems, measure their resilience, and manage their behavior during cyber incidents. A comprehensive strategy that considers the identification of those novel threats, detection and prevention methods will support the resilience, safety, and trustworthiness of digital health systems across Europe.

6) Promote AI for cyber security

AI technologies hold great potential to enhance cybersecurity in hospitals by enabling faster threat detection, real-time anomaly monitoring, and automated incident response. Promoting the development and adoption of AI-driven security tools can strengthen the ability of healthcare providers to anticipate, identify, and mitigate cyber threats more effectively, thereby improving overall protection of critical health infrastructure.

7) Establish structured exchange of lessons learned from cyber incidents

It is important to establish a formal mechanism, in cooperation with the European Health ISAC and national authorities, to facilitate the structured exchange of lessons learned from cyber incidents among hospitals and other healthcare providers. The anonymised case studies with technical details to incident port-mortems could valuably extend the envisaged cyber incident response playbooks and national cyber security exercises. Structured lessons learned could facilitate peer-to-peer learning mechanisms between hospitals and other healthcare providers interconnected for continuous healthcare delivery or located in a same local area or region.

8) Synchronise cyber security activities at EU level

At the time the action plan was published, there were already relevant working groups and formats, such as the European Health ISAC, the ENISA eHealth Expert Group, the eHealth Network and the ENISA eHealth Conference series; now, the action plan will create more. The tasks and scope of the formats should be clear, and duplication of work should be avoided.

9) **Strengthen cybersecurity workforce capacity**

Shortage of skilled personnel remains one of the main barriers to implementing cybersecurity measures in hospitals. The action plan should support workforce development through targeted training, certification programs, and knowledge exchange networks across Member States.

Kind regards

Prof. Dr. Michael Pilgermann | Prof. Patrizia Heinl | Prof. Dr. Andrius Patapovas