Official Journal
of the European Union

EN
C series

C/2025/4415

29.8.2025

Opinion of the European Committee of the Regions Cybersecurity of hospitals and healthcare providers

(C/2025/4415)

Rapporteur: Daniela CÎMPEAN (EPP/RO), President of Sibiu County Council

POLICY RECOMMENDATIONS

THE EUROPEAN COMMITTEE OF THE REGIONS (CoR)

1. Observes that cybersecurity efforts have not kept pace with the ongoing digital transformation in healthcare institutions and healthcare delivery, effectively turning healthcare into a prime target for malign actors;

2. Welcomes in this regard the publication of the Plan, recognising its timeliness and importance in the face of growing cyber attacks on European hospitals and healthcare providers;

3. Warns that cybersecurity threats have geopolitical implications and firmly believes that cybersecurity in healthcare is not just a technical issue but also a matter of local, regional, national and European security;

4. Warns that the rise in cybercrime, experienced since the outbreak of COVID-19 is not relenting; foreign-based and state-sponsored cyber-attacks not only focus on cyber espionage and intellectual property theft but also aim to destabilise whole societies;

5. Calls for 'cybersecurity by design' to be made a requirement by implementing proactive cybersecurity measures from the inception of new technologies for use in the healthcare sector, and strongly advocates ensuring that public healthcare providers purchase only mature products in terms of cybersecurity solutions, including backup and emergency systems that guarantee patient safety even in the event of network disruptions;

6. Highlights that in cases where attacks cannot be prevented, a dedicated rapid response service for the health sector may be available through the EU Cybersecurity Reserve established by the Cyber Solidarity Act. However, primary responsibility lies at local and regional level;

7. Supports the work carried out by the World Health Organization (WHO/Europe) on digital health and commits to working on this issue with the WHO, delivering on the jointly signed Action Plan 2025-2026;

8. Welcomes the 2025 WHO Europe guide on cybersecurity and privacy risk assessments in digital health, which provides a framework to help countries and organisations develop risk assessment strategies that align with their specific needs, goals and regulatory requirements;

9. Points to the growing impact of artificial intelligence (AI) both as a vector of threats (advanced phishing and deepfakes) and as a potential instrument for defence (detecting anomalies and providing automatic responses), and proposes that the action plan should tackle both aspects of AI;

On the regulatory framework

10. Emphasises that the action plan builds on the existing legislative framework in the field of cybersecurity – in particular the NIS2 Directive, the Cyber Solidarity Act (CSA), the Cybersecurity Act, the Medical Devices Regulation (MDR) and the Cyber Resilience Act; notes also the connection between the Plan and the draft Council Recommendation on the Union Blueprint for cybersecurity crisis management;

11. Warns that the evolving landscape presents complexities and overlaps between certification mechanisms under the CSA, the MDR, and the AI Act; this may lead to fragmentation and 'regulatory shopping', especially around voluntary participation schemes;

12. Supports the objectives of the EU-funded CYMDSEC project [1] to enhance cybersecurity in healthcare systems through comprehensive evaluation of device and network infrastructure design, cybersecurity, and regulatory frameworks;

13. Proposes to explore whether linking the requirements of the regulations for the application of the NIS2 Directive with those of Regulation (EU) 2016/679 on the protection of personal data could be beneficial to reduce administrative overlaps regarding the implementation of specific measures;

14. Points out that the gradual appearance of specific regulations is resulting in overlapping requirements which are difficult to follow and act on appropriately. Care must be taken to link up requirements and do away with overlaps from the very outset of the procedure for drawing up a new regulation;

On the Critical Entities Resilience Directive

15. Points out that the Critical Entities Resilience Directive (CER Directive), recognising health as a 'vital service for society and economy' and strengthening the resilience of critical infrastructure and critical entities against a range of threats, including cybercrime, entered into application on 18 October 2024;

16. Calls on the 24 Member States that received a formal notice at the end of November 2024 to immediately transpose the CER Directive into their national laws;

17. Calls on the European Commission to pursue infringement procedures where no satisfactory reply was received within the set deadline; considers the matter too important for European, national, regional and local security to be taken lightly;

18. Reminds the Member States that they are required to identify their critical entities for each sector (including health) set out in the CER Directive by 17 July 2026; and calls on Member States to accelerate the designation of critical healthcare entities and to provide them with concrete support in building their capabilities;

19. Is concerned that the vast majority of EU hospitals have never done a security risk assessment, as reported by the European Commission's DG CONNECT;

20. Is equally worried that only a quarter of the organisations surveyed in the preparation of the 2023 ENISA report had a dedicated ransomware defence programme;

21. Recognises that cyber regulation standards have been established in the past 5-6 years with the updated Network and Information Security Directive (NIS2), the Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), the Critical Entities Resilience (CER) and the AI Act; welcomes the Commission's intention to zoom in on hospitals and healthcare providers to improve their cyber resilience and recalls the importance of ensuring coherence and consistency between the various instruments while reducing overlaps;

22. suggests that Member States introduce regular, government-coordinated cyber incident exercises involving both national and regional healthcare actors;

On the NIS2 Directive

23. Points out that as of October 2024, the NIS2 Directive has officially become applicable, requiring hospitals, healthcare providers, medical device manufacturers and pharmaceutical companies to adopt robust cybersecurity measures;

[1] Homepage – Cymedsec.

24. Expresses concern that only six Member States have fully or partially enacted the directive into national law within the deadline;

25. Recognises that the implementation poses significant challenges, particularly for the healthcare sector, due to overlaps with existing regulations such as the Medical Devices Regulation, the European Health Data Space (EHDS) and the Cyber Resilience Act (CRA);

On the role of local and regional governments

26. Calls on the Commission to bear in mind that the management of health systems – and in particular hospitals – is decentralised to a greater or lesser extent in 19 out of the 27 Member States; is disappointed that the regional – and local – level are absent from the Communication; finds this omission troubling as it ignores the reality of ownership and stewardship of healthcare providers in two thirds of the EU Member States;

27. Calls on the Member States to fully involve their regions in the design and implementation of any cybersecurity strategies; points out that regional governments often lead on digital health initiatives and their expertise with the roll-out of e-health solutions might be vital to the successful introduction of new cybersecurity protocols and measures;

28. Underlines that beyond the question of decentralised management, healthcare systems across Europe are very different and include a range of organisations from fully public to fully private ones, including hybrid public-private partnerships; warns in this respect that public entities are often subject to budgetary restrictions and legal salary ceilings, making them less attractive as employers to cyber specialists;

29. Calls on the Member States to create networks of Regional Cybersecurity Support Centres for hospitals and healthcare providers to better connect local, national and European realities, with a particular focus on funding and attracting the talent needed to develop these centres;

30. Recommends involving regional and local government in the design of national action plans focused on cybersecurity in the health sector;

On costs and funding

31. Argues that cybersecurity spending will need to be systematically ring-fenced and normalised as part of the budgetary planning; hospitals and healthcare providers cannot haphazardly purchase disconnected protection 'gadgets'; instead, the protection of life-critical operational technology systems in healthcare needs to be regularly assessed, financed and implemented;

32. Draws attention to the challenge that managing and financing healthcare information and security systems poses to smaller regions;

33. Is appalled by the fact that the average cost of data leaks caused by ransomware attacks amounts to EUR 8 million, almost double the cost across other sectors;

34. Calls for greater clarity on the funding that should back up the ambitious goals laid out in the action plan; requests in particular detailed information on how local and regional government can finance the relevant digital transformation in healthcare;

35. Expects the Commission to clarify which actions should be financed by the Member States and which by the EU; for the latter, the CoR wishes to be informed on how the EU4Health and Digital Europe will interact in practice;

36. Warns that above and beyond investments in technology, funding must be channelled towards investments in shaping an organisational culture based on security at every level;

37. Deplores the deep cuts to the EU4Health budget in 2024 and calls on the Member States to protect it from future reductions; reiterates its position that health is not an expenditure but an investment into individual and collective well-being and resilience;

On cyber resilience in healthcare supply chains

38. Highlights that many hospitals and healthcare providers rely on outdated medical devices and software, which cannot withstand modern cyber attacks; recognises that in many places legacy solutions are indispensable for healthcare operations, yet risk becoming a significant vulnerability when they are no longer supported or maintained;

39. Calls for sustained and dedicated funding, both from national and EU sources, for hospitals to remove unsupported legacy technologies and to transition towards more secure and scalable cloud-based solutions;

40. Recommends aligning procurement processes with security standards and calls for specific guidelines detailing how to make compliance with cybersecurity benchmarks a prerequisite for participation in procurement tenders;

On the cybersecurity workforce

41. Reiterates the key messages of the CoR opinion on health workforce shortages and highlights that health systems face unprecedented acute and long-term shortages of key personnel; is concerned that balancing HR needs will become even more complex with the growing need to employ IT specialists and cybersecurity experts alongside the core medical staff;

42. Calls on public authorities, academia, VET institutions and NGOs to launch public campaigns to break down stereotypes about cybersecurity careers, to attract more women to the profession and to highlight the versatility of a cyber security career in healthcare;

43. Calls for an EU-wide training certification framework, enhancing the portability and recognition of cybersecurity in health skills;

44. Recognises that human error is a significant factor in data breaches, with individuals inadvertently falling for phishing scams, misconfiguring security settings or failing to follow established protocols; calls for training and risk awareness to be prioritised across the whole health sector; is convinced that cybersecurity cannot be a narrow confine of the IT department but a shared responsibility;

45. Recommends rolling out mandatory training designed to raise awareness about cybersecurity, to be flanked by result-oriented incentives, for all healthcare sector staff;

On specific elements of the action plan

46. Welcomes the idea of cybersecurity vouchers and calls on the Member States to introduce this measure to provide financial assistance to micro, small, and medium-sized hospitals and healthcare providers;

47. Highlights the fact that the Plan foresees that the Member States request that entities subject to the NIS2 Directive, including healthcare organisations, must report on ransom payments when reporting significant incidents to the competent authority under the NIS2 Directive; agrees that such reporting would improve data collection and assessment of the effectiveness of measures taken against ransomware attacks; calls however for more details on how this reporting would be operationalised given that it is not mandatory under the NIS2 Directive;

48. Notes that the action plan calls for manufacturers of medical and in vitro diagnostic devices to voluntarily report actively exploited vulnerabilities or severe cyber incidents impacting on the security of their products; highlights that these manufacturers fall outside the scope of the Cyber Resilience Act and recommends that the ongoing evaluation of the regulations addresses better coherence between the regulatory frameworks;

49. Supports the idea of creating a European Health CISO (Chief Information Security Officer) Network so that experts can share best practices, including talent retention strategies and solutions for attracting cybersecurity professionals to the healthcare industry; calls on the Commission and the Member States to make sure that experts nominated by regional government are also welcome to join the network;

50. Welcomes the establishment of the European Cybersecurity Support Centre for hospitals and healthcare providers within ENISA; notes the significant number of tasks that the new support centre is set to perform and calls on the Commission to provide further information on the composition and the financing of the centre;

51. Calls on the Commission to involve the regional and local governments in the development of a 'user-friendly, easy access' repository of all available instruments for preparedness, prevention, detection and response; the repository, created by the support centre, should cover tools and policies from all governance levels;

On trust and privacy

52. Argues that security and privacy are intertwined: security measures protect data confidentiality, integrity and availability, which are foundational to privacy. At the same time, privacy regulations often mandate specific security controls to protect personal data. Protecting privacy builds patient trust and cybersecurity awareness, ensuring that sensitive health information is handled with care;

53. Draws attention to the 2024 ENISA Report on the State of Cybersecurity in the Union and its findings that the EU health sector's cybersecurity maturity is 'moderate' with wide differences in the level of cybersecurity maturity between healthcare entities across Europe; underlines that patients' data must be protected to ensure their continuous trust in the European Health Data Space;

54. Considers that delivering on the European Health Data Space (EHDS) will require more focus on securing national and cross-border interconnection infrastructure, such as National Contact Points for eHealth. This infrastructure is becoming critical for large-scale data protection and the Committee considers that specific measures for it must be drawn up in consequence.

Brussels, 3 July 2025.

The President
of the European Committee of the Regions
Kata TÜTTŐ