Council of the European Union

Brussels, 16 January 2025
(OR. en)

5426/25

CYBER 21
SAN 15

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 January 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2025) 10 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European action plan on the cybersecurity of hospitals and healthcare providers

Delegations will find attached document COM(2025) 10 final.

Encl.: COM(2025) 10 final

EUROPEAN
COMMISSION

Brussels, 15.1.2025
COM(2025) 10 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

European action plan on the cybersecurity of hospitals and healthcare providers

1. Introduction

The EU's security environment is rapidly changing, with an escalation of hybrid attacks and cyberattacks that aim to destabilise our society, seeking division and disruption but also profits from cybercrime. Europe must therefore urgently strengthen its preparedness for and resilience against this new reality, across all sectors and in line with a 'whole-of-society' and 'whole-of-government' approach, as called for in the report by the Special Adviser to the President of the European Commission, Sauli Niinistö.

Secure and resilient healthcare systems are a cornerstone of the EU's social model. However, hospitals and healthcare systems are facing mounting threats, particularly from ransomware gangs targeting them for financial gain, driven by the high value of patient data, including electronic health records. The health sector has indeed become the most attacked industry in the EU over the past four years, including during the COVID-19 pandemic when health infrastructure was increasingly targeted by cyberattacks. Cyberattacks on hospitals and healthcare providers are causing direct harm to people, delaying medical procedures, causing gridlocks in emergency rooms and could, in extreme cases, lead to the loss of life.

The stakes are even higher as the sector undergoes a vital digital transformation. Digital health and the use and reuse of health data can enable models of care better suited to people and patients' needs and preferences, by preventing the onset of disease or enabling earlier treatment. The integration of digital tools and solutions in clinical processes as well as the use and reuse of health data can inform better clinical decisions, contribute to automation in health as well as to faster and better patient care. Digital tools, data usage, and medical devices – which are often connected to the internet and powered by artificial intelligence (AI) – are also key to address challenges such as the shortage of healthcare professionals.

At the same time, digital tools also expand the potential targets for cybercriminals. Moreover, certain state actors do not shy away from targeting healthcare facilities, as witnessed by Russia's ongoing war of aggression against Ukraine. This makes the sector a potential target for cyberattacks as part of a wider hybrid campaign. Cyberattacks not only jeopardise patient safety but also erode public trust in health infrastructure and come with significant recovery costs. Beyond guarding against cyberattacks, a resilient and secure digital infrastructure is also essential for supporting the implementation and full deployment of the European Health Data Space[1] (EHDS).

Therefore, it is time to level up and strengthen the cybersecurity and resilience of Europe's hospitals and healthcare providers, as emphasised by President von der Leyen in her Political Guidelines for the 2024-2029 Commission[2]. This action plan responds to the urgency of the situation and the unique threats facing the sector. There is no simple 'silver bullet' solution to the cybersecurity challenges in healthcare. Instead, the action plan calls for strengthened prevention, preparedness, and a more coordinated approach to solidarity while tapping into the expertise of the European cybersecurity industry. As such, the action plan reflects the EU approach to security that will be further developed and formalised in the upcoming European Internal Security Strategy, defining comprehensive response to face all internal security threats

[1] https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/
[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

and focussing on the capacity to anticipate threats, to prevent harm and protect people, acting at all levels with a whole-of-society approach.

The health sector includes a broad number of entities and actors, comprising hospitals, clinics, care homes, rehabilitation centres and various healthcare providers, alongside the pharmaceutical, medical and biotechnology industry, medical devices manufacturers, and health research institutions. This action plan predominantly focuses on the cybersecurity of hospitals and healthcare providers, understood as any natural or legal person – or any other entity – legally providing healthcare on the territory of a Member State[3]. Hospitals and healthcare providers are interdependent with other health entities, and they are closest to people. At the same time, measures to enhance the cybersecurity of hospitals and healthcare providers should also address risks affecting the broader supply chain and ecosystem, stemming for instance from entities that use health data for research and machine learning or that produce medical devices, in particular digitally enabled medical devices that connect to the internet or other devices ("internet of things").

While securing health systems is primarily a national competence, health is also a critical sector under the Directive on measures for a high common level of cybersecurity across the EU (NIS2)[4]. Cybercriminals and other threat actors operate across borders, and the cybersecurity challenges faced by healthcare organisations are also similar across Member States. Cooperation at the European level is valuable for sharing and scaling up best EU-level and national practices. Therefore, the Action Plan proposes EU-level coordination and measures, whilst also calling on Member States to take action to make a difference for healthcare and the wider health ecosystem.

The focus of the Action Plan is on building the sector's capacities to **prevent** cybersecurity incidents in the first place, because prevention is always better than the cure. Secondly, the Action Plan details actions to improve cybersecurity information-sharing and capability to **detect** cyber threats, allowing a faster reaction. Thirdly, it provides measures to better **respond** to incidents, and to **recover** from them. Finally, the Action Plan envisages ways to **deter** cyber threat actors from launching attacks against health systems in Europe.

The Action Plan will be implemented hand in hand with healthcare providers and the wider health ecosystem, Member States, and the cybersecurity community. A collaborative approach is key to further defining and refining the most impactful actions so that all of Europe's critical healthcare providers can benefit from them. Therefore, this Communication will be accompanied by the launch of a comprehensive consultation with stakeholders, industry and Member States.International cooperation is important for cybersecurity due to the borderless and interconnected nature of cyberthreats. Comparable cybersecurity threats are present also in the enlargement and neighbourhood countries and other EU strategic partner countries. This can ultimately endanger the security of critical infrastructure in the EU. It will therefore be important to reflect the lessons learned from implementing the Action Plan also in

[3] Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0024

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), https://eur-lex.europa.eu/eli/dir/2022/2555

the EU's cooperation with both enlargement and other partner countries, in light of the threat levels to which they are respectively exposed.

2. Cybersecurity challenge of hospitals and healthcare providers

Cyber threats to the health sector

Cyberattacks are on the rise globally and within the EU, with an increasingly complex and dynamic threat landscape. Advancements in AI are equipping criminal and malicious actors with powerful tools to increase the precision and impact of their operations, while, at the same time, reshaping cyber defence possibilities by allowing automated and real-time action against attacks.

Ransomware remains a critical cybersecurity challenge in the EU and globally, with one report estimating a global annual cost of more than EUR 250 billion by 2031[5]. When ransomware criminals strike, they not only encrypt victims' data for ransom but increasingly leak sensitive information to exert additional pressure. Another prominent challenge is vulnerabilities in software and hardware: according to the European Union Agency for Cybersecurity (ENISA)[6], healthcare is the sector that declared the most security incidents related to such vulnerabilities.[7] Other growing threats include distributed denial-of-service (DDoS) attacks, designed to overwhelm a targeted system with a flood of traffic, rendering it inaccessible to legitimate users[8].

The health sector faces similar cybersecurity threat trends, with a pronounced emphasis on ransomware attacks. According to the ENISA, ransomware accounted for 54% of analysed cybersecurity incidents in the health sector in 2021–2023. 83% of attacks were financially motivated, driven by the high value of healthcare data, while 10% of attacks had an ideological motivation[9]. Similarly, a 2024 report by the Commission found that 71% of attacks with effects on patient care, such as delayed treatment, diagnosis and impaired access to emergency services, were of the ransomware type[10]. Ransomware attacks can have a particularly disruptive effect on the provision of healthcare services, putting patient safety at risk.

---

[5] Cybersecurity Ventures (1 June 2024): "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031". Available at https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[7] ENISA Threat Landscape: Health Sector (July 2023).

[8] ENISA Threat Landscape 2024.

[9] ENISA Threat Landscape: Health Sector (July 2023). The report analysed healthcare providers, as well as other types of organisations including organisations conducting health-related research, entities manufacturing certain health-related products, health authorities, health insurance organisations, and residential treatment facilities and social services providers. Available at https://www.enisa.europa.eu/publications/health-threat-landscape

[10] European Commission: Joint Research Centre, Reina, V. and Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Publications Office of the EU, 2024, https://data.europa.eu/doi/10.2760/693487

Moreover, ransomware attacks are often coupled with breaches of patient data[11], which often includes sensitive health-related data and violates people's fundamental right to protection of personal data.

At the same time, with the increasing digitalisation of healthcare, the attack surface is growing. According to the Report on the State of the Digital Decade 2024, an average of 79% of EU citizens have online access to their electronic health records in primary care[12]. Electronic health records, clinical information systems, hospital workflow systems, IT systems for handling reimbursement of treatments, medical imaging systems, and medical devices used for diagnostic purposes or for patient monitoring are all examples of digital tools that can play a major role in boosting the efficiency and performance of the health sector, but are also potential targets of a cybersecurity attack. Specific healthcare activities such as intensive care and radiological imaging, or medical fields such as oncology and cardiology, that are highly dependent on digitally enabled devices, are at a particular risk of cyberattacks. In addition, supply chain issues may lead to the procurement of devices with insufficient cyber security, exacerbating existing general risks.

For example, during the COVID-19 pandemic, a ransomware attack paralysed large parts of the Irish health care system, leading to cancellation of at least some services at 31 of the 54 acute hospitals on the morning of the incident.[13] Health services had to revert to paper records, slowing down the efficiency of operations. The attack originated from a phishing email containing a malicious attachment.[14] The incident demonstrated the potential of cyberattacks spreading across different systems, and consequently the importance of protecting the entirety of a healthcare organisation's attack surface. It also underlined the importance of ensuring fundamental cyber hygiene and cybersecurity culture throughout organisations.

Cybersecurity maturity of hospitals and healthcare providers

The healthcare landscape in the EU is very diverse, with hospitals and other healthcare providers varying greatly in terms of ownership, structure and size across Member States. In some cases, healthcare governance can be based on a centralised approach at national level, in others at regional and local level; healthcare providers can be publicly or privately owned. Furthermore, differences can also exist within the same country, for example where there are significant socio-economic and territorial disparities across regions, leading to a complex picture. This complex healthcare landscape can be challenged by important health crises, due to communicable diseases, such as the COVID-19 pandemic, but also other health risks for instance related to climate change. Finally, there is significant variability and fragmentation in the level of digitalisation and adoption of technology by healthcare providers. An example of this complexity is that service unavailability caused by a cybersecurity incident can result in

[11] According to the ENISA Threat Landscape for the Health Sector, breach or theft of data was confirmed in 43% of ransomware incidents analysed.
[12] Report on the State of the Digital Decade 2024
[13] Irish Health Service Executive (2021): 'Conti cyber attack on the HSE: Independent Post Incident Review'.
[14] Irish Health Service Executive: 'Cyber-attack and HSE response'. Available at https://www2.hse.ie/services/cyber-attack/what-happened/.

serious damage and harm to patients even in small-scale healthcare facilities, including clinics or emergency medical services which provide an essential service to a relatively low number of users.

According to the 2024 ENISA Report on the State of Cybersecurity in the Union[15], the EU health sector's cybersecurity maturity is moderate and there are wide differences in the level of cybersecurity maturity between healthcare entities across Europe. Deficiencies can be observed in key areas such as sufficient human resources, organisations' knowledge of their information and communications technology (ICT) supply chains, and installation of up-to-date security features in products. The sector struggles with basic cyber hygiene and fundamental security measures, as illustrated by the fact that nearly all health organisations surveyed face challenges when it comes to performing cybersecurity risk assessments, while almost half have never performed a risk analysis.[16]

Another significant challenge for the cybersecurity of hospitals is the intersection of information technology (IT) and operational technology (OT), where different security priorities meet as regards confidentiality, availability and reliability, and where a breach in one area can affect the other. The 2024 ENISA Report on the State of Cybersecurity in the Union further stresses that the health sector is not performing adequately in ensuring the security of the ICT products and processes it uses, due to the large variety of health entities, devices and products.

This diversity, combined with varying levels of cyber awareness among hospital staff and management, creates a complex challenge for ensuring the cybersecurity of healthcare systems. For instance, according to the 2024 Eurobarometer on Cyberskills, only 25% of surveyed companies in the health, education and social care sector had provided training or awareness-raising about cybersecurity in the previous 12 months[17]. Action is needed to foster a culture of cybersecurity awareness among frontline healthcare professionals. For example, staff rotations, use of shared workstations, poor authentication management and the use of removable media are additional sources of vulnerabilities affecting healthcare providers' cybersecurity[18].

In many cases, IT and OT are at least partly outsourced. The 2024 Eurobarometer found that the share of companies outsourcing at least some aspects of their cybersecurity is the highest in the health, education and social care sector, with 57% of surveyed companies doing so[19]. Similarly, there is a strong trend of migrating to cloud computing, driven by the need for scalable data storage and management, cost efficiency, improved collaboration, and support for advanced technologies like AI and the Internet of Medical Things. In 2022, 58% of health organisations used a cloud-based digital health platform[20].

---

[15] ENISA: 2024 Report on the State of Cybersecurity in the Union (September 2024). Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[16] ENISA Threat Landscape: Health Sector (July 2023). Available at https://www.enisa.europa.eu/publications/health-threat-landscape

[17] Flash Eurobarometer 547 on Cyberskills (May 2024). Available at https://europa.eu/eurobarometer/surveys/detail/3176

[18] Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.

[19] Flash Eurobarometer 547 on Cyberskills.(May 2024). Available at https://europa.eu/eurobarometer/surveys/detail/3176

[20] ENISA: NIS Investments Report 2022 (November 2022). Available at https://www.enisa.europa.eu/publications/nis-investments-2022

However, while this shift can bring significant efficiencies, it also entails risks that require informed decisions about procurement and secure configuration.

Overarching all of these challenges is the question of capacity building and funding. Funding for cybersecurity in the health sector has been limited and remains a universal challenge across the EU[21]. Furthermore, these funding challenges arise against the background of an ageing population, which is expected to create widespread budgetary pressures on Europe's health systems in the coming decades.

The continued use of obsolete tools and legacy systems, limited resources to prevent or react to incidents, and gaps in cybersecurity maturity often stem from funding shortfalls. Hospitals face a continuous challenge to balance an up-to-date secure and digital infrastructure with other necessary investments to improve patient care, such as hiring of doctors and other healthcare professionals, implementation of novel diagnostic and treatment methods, and acquisition of devices. According to ENISA[22], the health sector ranks only 7th of the 12 sectors studied when it comes to the proportion of information security spending out of the total IT spending, with 8.3% being the median in the health sector.

3. European Cybersecurity Support Centre for hospitals and healthcare providers

The EU's cybersecurity framework offers a broad range of tools that should be leveraged to improve the security and resilience of hospitals and healthcare providers. To address the numerous challenges highlighted above, it is necessary to develop a unified, strategic approach at EU level, bringing together the necessary resources, expertise, and tools to effectively tackle cyber threats. A comprehensive overview, as well as better planning and coordination, are essential to help healthcare providers across the EU strengthen their defences. To achieve this, ENISA is best placed to establish, within its organisation, a dedicated **European Cybersecurity Support Centre for hospitals and healthcare providers**[23] as part of its mandate[24] to safeguard and support the EU's critical infrastructure.

The Support Centre should progressively **develop a comprehensive service catalogue catering to the needs of hospitals and healthcare providers**, outlining the range of available services for preparedness, prevention, detection and response. Working with Member States' authorities and drawing from the experiences of hospitals and healthcare providers, the Support Centre should develop a user-friendly, easy-access repository of all available instruments at European, national and regional levels. In conducting its activities, it should ensure proper coordination with Member States, and support prioritisation and delivery of actions as needed in real time.

As an important building block for the development of the service catalogue of the Support Centre, the Commission will propose to launch pilots across the EU to develop best practices for cyber hygiene and

[21] The organisation and delivery of health services and medical care is a national competence under Article 168 Treaty on the Functioning of the European Union, and financing of healthcare systems varies across Member States.
[22] ENISA: NIS Investments Report 2022 (November 2022). Available at https://www.enisa.europa.eu/publications/nis-investments-2022.
[23] In this document, "Support Centre" is used interchangeably.
[24] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.

security risk assessment, as well as addressing the need for continuous cybersecurity monitoring, threat intelligence and incident response using state-of-the-art cybersecurity solutions. Outcomes of these pilots, which will be funded by the Digital Europe Programme, executed by the European Cybersecurity Competence Centre (ECCC), will inform further actions at the EU level including the work of the Support Centre.

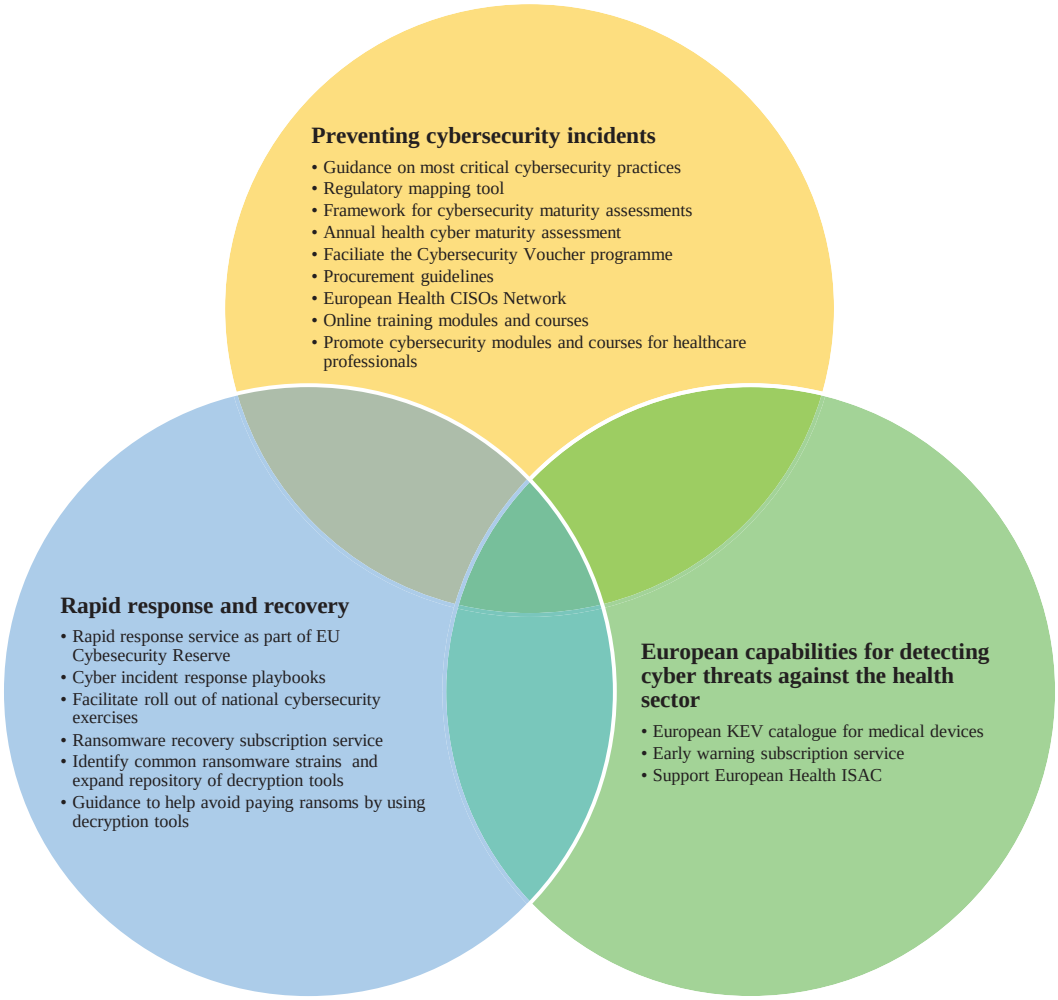

Figure 1: Concepts for the Support Centre's service catalogue for hospitals and healthcare providers

3.1. Preventing cybersecurity incidents

Simple actions that shift the odds

Basic cybersecurity measures, such as ensuring that systems are kept up to date, managing backups, and implementing multi-factor authentication can, according to one estimate, protect organisations from up to 98% of attacks[25]. Many of the most impactful cyber hygiene and risk-management measures are relatively straightforward to adopt, making them a low-hanging fruit for improving cybersecurity. One of the key roles of the Support Centre should therefore be to **develop clear, targeted guidance that highlights the most critical cybersecurity practices and aids healthcare providers in implementing them**. This support must extend beyond large hospitals to include tailored advice for smaller entities, such as local General Practitioner's offices and specialist clinics, which often lack the resources for dedicated cybersecurity teams but remain equally vulnerable to attacks. Furthermore, it is necessary to consider the regional importance of specific healthcare entities for ensuring patient care, for instance in sparsely populated areas. Health research institutes that handle large amounts of sensitive personal data could also benefit from receiving guidance on basic cybersecurity measures to enhance their resilience.

Healthcare organisations are also subject to a range of cybersecurity-related obligations stemming from EU legislation[26]. While the obligations are crucial for ensuring a high common baseline for cyber and data security, it is essential to ensure that the regulatory landscape is not needlessly difficult and burdensome to navigate. A heavy focus on compliance should not run counter to the objective of fostering a strong cybersecurity culture. An **easy-access regulatory mapping tool can help minimise the administrative burden for entities subject to multiple regulatory instruments**. Along with

[25] Microsoft Digital Defense Report 2022. Available from https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Such as the NIS2 Directive; Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/enghttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, https://eur-lex.europa.eu/eli/reg/2017/745/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (Medical Devices Regulation), https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng, the Medical Device Regulation; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices (In vitro diagnostic medical devices Regulation), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space, COM(2022)197 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197. Negotiations concluded with a political agreement in spring 2024 and, following finalisation, publication in the Official Journal is expected for spring 2025

developing guidance and toolkits, the Support Centre should work closely with the Commission and Member States to develop and disseminate such a tool as soon as possible. The Support Centre would therefore play an important role in making cybersecurity rules simple to understand and to implement, for instance by providing implementation guidance[27] and where necessary promoting relevant standards.

The forthcoming **European Digital Identity Wallets** are another tool for facilitating simple implementation of good cyber hygiene practices. Reducing the reliance on weak identification mechanisms, such as passwords, is essential to mitigate the risks of unauthorised access to health data. A shift towards secure sign-on solutions based on reliable identification is critical. The EU Digital Identity Wallet offers a harmonised, EU-wide approach to electronic identification for healthcare professionals, providing a robust and unified solution as of end of 2026. All online health information systems required to implement strong user authentication will be obliged to accept the Wallet for identification purposes as of the end of 2027[28].

Preparedness and Targeted Support

Preparedness testing, involving actions such as penetration testing, is a cornerstone of effective cybersecurity, and the Commission has already allocated funding to ENISA for pilot preparedness initiatives, which revealed that the health sector is among the most in-demand areas for testing and further assessments to identify gaps in cybersecurity maturity. With the entry into force of the Cyber Solidarity Act, these efforts will expand significantly, with the ECCC taking the lead . To address this need, the Commission will propose, in consultation with the NIS Cooperation Group, EU-CyCLONe[29] and ENISA, to identify health as a sector for which support can be given for **coordinated preparedness testing** under the Cyber Solidarity Act. Furthermore, the Support Centre should develop a **tailored framework for cybersecurity maturity assessments specific to healthcare**. Such maturity assessments would provide entities with actionable insights into their vulnerabilities while allowing them to demonstrate their cybersecurity readiness to patients and stakeholders, building trust in their services. At an aggregated level, the Support Centre should carry out an **annual Health Cyber Maturity Assessment**, which would establish a clear overview of the health sector's cybersecurity at both national and EU levels.

The health sector relies heavily on external contractors for cybersecurity services[30], highlighting the need for targeted support to strengthen defences. Building on successful initiatives such as the EU Innovation Vouchers, the **Member States should consider targeted measures like Cybersecurity Vouchers for micro, small, and medium-sized hospitals and healthcare providers**. These vouchers would provide

[27] The development of guidelines on the interpretation of the General Data Protection Regulation (GDPR) falls within the responsibility of the European Data Protection Board (EDPB). The development of guidance by ENISA should fully respect the EDPB's prerogatives.
[28] Article 5(f)(1)–(2) of Regulation (EU) 910/2014.
[29] European cyber crisis liaison organisation network
[30] See the ENISA NIS Investments Report 2023 (November 2023), highlighting prominence of external support for cybersecurity auditing and compliance. Available at https://www.enisa.europa.eu/publications/nis-investments-2023

financial assistance to put in place specific cybersecurity measures. The prioritisation of the allocation of vouchers should be informed by the findings of preparedness testing and maturity assessments.

Local knowledge and context are crucial for the effective rollout of vouchers or other support programmes, ensuring relevance and accessibility. EU funds, such as the European Regional Development Fund, are already active in supporting cybersecurity and digital health initiatives, and could therefore serve as a vehicle to develop targeted cybersecurity voucher schemes for healthcare providers. To drive this effort, the Support Centre would collaborate with Member States and regional programme authorities to support the development of such regional voucher schemes, drawing on lessons from existing national projects as well as actions funded under Digital Europe Programme to ensure practical and impactful implementation.

Furthermore, since 2014, the Horizon programmes have been instrumental in funding a range of research initiatives focused on enhancing the resilience of healthcare institutions, such as hospitals, against cyber threats and mitigating the risks associated with the misuse of emerging technologies. The resulting deliverables include a suite of specialised tools, frameworks, and systems, such as risk assessment tools, privacy-preserving data-sharing platforms, cryptographic solutions, cybersecurity awareness training programmes, and real-time threat detection systems. Notably, these solutions have been rigorously validated through real-world pilot implementations in healthcare environments, ensuring their effectiveness and practical applicability in protecting against cyber threats.

Securing Healthcare Supply Chains

A key challenge for healthcare organisations is managing complex ICT supply chains, which involve a range of products such as connected medical devices, Electronic Health Records systems and office hardware. Hospitals and healthcare providers need reliable and secure ICT systems and services for their operations. To help address cybersecurity challenges in the health sector, the NIS Cooperation Group should perform a **coordinated security risk assessment, assessing both technical and strategic risks related to medical devices supply chains and proposing mitigating measures.**[31] As appropriate, the NIS Cooperation Group should collaborate with the Medical Device Coordination Group.

The Cyber Resilience Act is a new, comprehensive framework that sets cybersecurity requirements for planning, design, development, as well as handling, patching, and reporting of actively exploited vulnerabilities regarding almost all hardware and software products, at each stage of the value chain[32]. Medical devices are a type of product used in one of the most sensitive areas of our society. The cybersecurity requirements for these products stem from the pre-existing Medical Devices Regulation

[31] Pursuant to Article 22 of the NIS2 Directive.

[32] In a first step, as of 1 August 2025, broad categories of radio equipment, not falling within the scope of the Medical Device Regulation and the Regulation on in vitro diagnostic medical devices, will be required to comply with the essential requirements of the Radio Equipment Directive that relate to cybersecurity when they are placed in the Single Market. In a second stage, as of 11 December 2027, the Cyber Resilience Act will enter into application.

and the Regulation on in-vitro diagnostic medical devices[33]. The ongoing evaluation of those regulations is examining the potential for greater coherence and synergies between these frameworks in order to guarantee simplification and state-of-the-art cybersecurity.

Furthermore, the findings of the risk assessment should support healthcare organisations in reviewing their supply chain cybersecurity practices as required under the NIS2 Directive, and could inform the development of new **Procurement Guidelines**[34]. Developed by ENISA through its Support Centre, these guidelines should reflect recent trends, such as cloudification of patient data storage, including the need for secure migration of electronic health data to cloud environments. Moreover, the new Guidelines should offer practical tools for organisations to keep track of their supply chains, including managed security service providers (MSSPs), attestation reports or third-party risk assessments.

For cloud, further action is needed to address the unique challenges of managing sensitive healthcare data, including heightened security, privacy, and operational risks. To strengthen safeguards, experts recommend embedding "Security by Default and by Design" into cloud services. This approach prioritises secure infrastructure, proactive vulnerability management, and a mix of governmental and private cloud solutions. Continuous monitoring and vendor-specific attestations—such as security provider certifications and compliance audits with national and international standards—are also essential for ensuring robust security practices.

For services like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), security implementation often falls to the customer. However, many healthcare organisations lack the resources to meet these requirements independently. To address this, **cloud service providers should be encouraged to implement baseline security measures as a standard feature**. These measures would reduce the risk of misconfigurations, maintain consistent protection across customer-managed environments, and provide greater assurance to users. Establishing a default security baseline would aim to balance robust protection with practicality, ensuring usability for a wide range of healthcare organisations. This effort would involve close collaboration between cloud providers and the health sector, leveraging industry best practices to create effective and scalable solutions.

Training and skills development

Having a workforce with in-demand skills is important for long-term sustainable growth and competitiveness in Europe, as well as for high-quality services, including healthcare services. The shortage of qualified cybersecurity professionals is a significant challenge across Europe, with an estimated gap of 299,000 professionals to fill workforce needs in the EU[35]. According to the 2024

[33] In December 2019, the Medical Devices Cooperation Group issued guidance on cybersecurity for medical devices, supporting manufacturers in fulfilling the requirements of Annex I of the two Regulations: https://ec.europa.eu/docsroom/documents/41863.

[34] Building on the 2020 ENISA Procurement Guidelines for Cybersecurity in Hospitals (February 2020). Available at https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform

Eurobarometer on Cyberskills[36], 81% of companies view difficulties in hiring cybersecurity staff as a key risk for potential cyberattacks. In the education, health, and social work sectors, 66% of cybersecurity roles are filled by employees transitioning from non-cybersecurity positions, highlighting the urgent need for reskilling and upskilling.

To address this challenge, the Support Centre should collaborate with the future cybersecurity skills European Digital Infrastructure Consortium (EDIC) foreseen in the Commission Communication on the Cybersecurity Skills Academy[37]. The work should facilitate exchanges among cybersecurity professionals in the health sector, such as Chief Information Security Officers (CISOs). One potential action would be to create a **European Health CISOs Network** , starting with a pool of experts to share and develop best practices, talent retention strategies, and solutions for attracting cybersecurity professionals to the health sector. Furthermore, under the umbrella of the Cybersecurity Skills Academy, resources should be developed to enhance the cybersecurity workforce in the health sector with the support of industry and academia. In this regard, industry stakeholders should be encouraged to pledge support for enhancing cybersecurity training.

Human error continues to be a major contributor to cybersecurity incidents in healthcare, underscoring the critical need for comprehensive staff training and cyber awareness. Given the frequent use of digital tools by healthcare professionals, it is vital to equip them with the knowledge of secure practices. Targeted training and awareness campaigns can significantly reduce risks. To address this, the Support Centre should work with healthcare professionals and providers, and cooperate with education and training providers, industry, the cybersecurity skills EDIC as well as Member State authorities to create and disseminate **extensive, easy-to-access online training modules and courses**.

Incorporating digital competence and cybersecurity modules into educational curricula is crucial for building a strong cybersecurity foundation in healthcare. These modules should address sector-specific issues like patient-data protection and vulnerabilities in the security of medical devices. The development of these resources should take into account prior actions, such as the BeWell project funded under the Erasmus+ programme[38] and the PANACEA project funded under Horizon 2020[39].

3.2.European capabilities for detecting cyber threats against the health sector

Effective cyber threat detection is essential for prompt response to incidents. Threat actors can leverage techniques to make intrusions difficult to detect, enabling extended periods of unpermitted access to a

[36] Flash Eurobarometer 547 on Cyberskills.
[37] Communication from the Commission to the European Parliament and the Council: Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'). COM(2023) 207 final.
[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. Available from https://bewell-project.eu/.
[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people. Available from https://cordis.europa.eu/project/id/826293.

system[40]. Therefore, better threat detection capabilities can help stop cyberattacks in their tracks. For example, in the ransomware attack against the Finnish psychotherapy service provider Vastaamo, during which the perpetrator extorted patients whose confidential patient records were stolen, the initial intrusion occurred in 2018, but only became known to the provider in 2020[41].

Efficient information sharing and collaboration are essential for enhancing threat detection and situational awareness throughout the EU. Computer Security Incident Response Teams (CSIRTs) play a vital role in receiving reports of incidents, near misses and potential threats, offering guidance on mitigation measures at the national level. However, **Member States are strongly encouraged to also share all cyber incident notifications from hospitals and healthcare providers with ENISA's Support Centre to allow for EU situational awareness**. Ideally, this should be accompanied by a meaningful characterisation of various relevant incident dimensions, including known root vulnerabilities and effects on healthcare services and patient adverse events. Furthermore, manufacturers of medical and in vitro diagnostic devices are encouraged to voluntarily report, via the single reporting platform to be established and managed by ENISA within the framework of the Cyber Resilience Act, actively exploited vulnerabilities or severe cyber incidents having an impact on the security of these devices, as well as potentially other vulnerabilities, incidents, near misses or cyber threats that may affect the risk profile of these devices.

Where the information contained in the reports is no longer sensitive, the Support Centre could build up an ENISA-sponsored European known exploited vulnerabilities (KEV) catalogue for medical devices, electronic health record systems and providers of ICT equipment and software in health. To address significant challenges of threat detection, the Support Centre should introduce **an EU-wide early warning subscription service for the health sector, delivering near-real-time alerts**. This service would draw on processed data from CSIRTs, healthcare entities and manufacturers, Open-Source Intelligence (OSINT), and other relevant actors such as Cyber Hubs, Information Sharing and Analysis Centres (ISACs) and law enforcement authorities. Enhanced cooperation between ENISA and the European Union Agency for Law Enforcement Cooperation (Europol) – for example on patterns of cybercrime against the health sector – would further boost situational awareness.

ISACs serve as central resources for cyber threat intelligence, fostering two-way information sharing between the public and private sectors, and promoting trust-building. The Support Centre should step up support for the **European Health ISAC** with tools and information exchange, sectorial situational awareness reports, as well as fostering a trusted community for tactical and strategic collaboration. Member States should encourage the development of national health ISACs[42]. The ISACs should also be encouraged to bring together healthcare providers with manufacturers to give rise to a joint understanding of cybersecurity threats, including in the supply chain, and facilitating a dialogue about secure design of products that truly take into account the deployment realities on the ground.

[40] ENISA Health Threat Landscape 2023.
[41] Decision 1150/161/2021 of the Finnish Data Protection Ombudsman.
[42] For example, Finland has a national ISAC for the social welfare and health care sector. See Finnish National Cybersecurity Centre: 'ISAC information sharing groups', available at https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

3.3.Rapid response and recovery

Given the high sensitivity of patient health data and the potentially devastating effects of cyberattacks on healthcare services, a swift and effective response to cybersecurity incidents is crucial to safeguarding patient safety. When a hospital or healthcare provider faces a cyberattack, the first point of contact is the relevant national CSIRT[43]. The CSIRT is responsible for providing timely support, ideally within 24 hours, to help manage significant incidents. However, if an incident exceeds the CSIRT's capacity, EU support should be available to ensure a swift and effective response.

The EU Cybersecurity Reserve, established under the Cyber Solidarity Act, provides incident response services from trusted managed security providers to assist with significant or large-scale cybersecurity incidents and initial recovery efforts. This reserve is designed to complement the efforts of Member States' CSIRTs, enabling them to request additional support in cases involving critical sectors like health. To enhance this system, the **Commission and ENISA should ensure that the Reserve includes a Rapid Response Service specifically for the health sector.** In complementarity with other existing frameworks, this service would deploy experts to manage significant or large-scale cybersecurity incidents in healthcare without delay when national support is insufficient.

To improve response and recovery, the Support Centre, in collaboration with the NIS Cooperation Group, the CSIRTs Network and, where relevant, Europol, should develop **cyber incident response playbooks tailored for healthcare**. These playbooks would guide both CSIRTs and healthcare organisations in responding to specific cybersecurity threats, including ransomware. Given the importance of effective cooperation among CSIRTs and law enforcement authorities in responding to and investigating cybersecurity incidents of criminal nature, the playbooks should, among other aspects, provide clear guidance on the reporting of such incidents to law enforcement. Furthermore, the Support Centre could **facilitate a wide roll-out of national cybersecurity exercises, building on experiences from exercises like ENISA's Cyber Europe 2022 exercise, to test the playbooks and strengthen incident response protocols.**

To inform policies and assess the effectiveness of measures taken against ransomware attacks, it is necessary to collect further data. To this effect, Member States should request entities subject to the NIS2 Directive, including healthcare organisations, to report on any ransom payments made and on ransom payments they intend to make, alongside other information they provide when reporting on significant cybersecurity incidents. Such reporting supports the effective investigation of ransomware incidents, including the tracing of payments on cryptocurrency exchange platforms in order to identify the recipients.

Recovery speed is a critical factor in maintaining resilience and public trust, particularly in healthcare, where downtime can disrupt patient care. For effective recovery from ransomware attacks, healthcare

[43] Article 23(1) of the NIS2 Directive sets a requirement for essential and important entities to notify significant incidents to the relevant CSIRT or, where applicable, competent authority.

providers must have secure, up-to-date, and isolated backups that can be quickly restored. As part of its service catalogue, the Support Centre could offer **a ransomware recovery subscription service, helping hospitals and healthcare providers prepare recovery plans in advance**. ENISA and Europol should collaborate to identify the most common ransomware strains targeting healthcare organisations and **expand the repository of decryption tools** available through the No More Ransom project[44]. They should also develop and promote accessible guidance to help healthcare providers avoid paying ransoms by using decryption tools.

The **International Counter Ransomware Initiative**[45] is a valuable arena for exchange on specific ransomware incidents, as well as for building the capacities of member countries to strengthen their cybersecurity frameworks and investigation capabilities against ransomware actors. The Commission, working together with the High Representative, will continue to advance cooperation in the Counter Ransomware Initiative, including against ransomware threats to the health sector. Moreover, the Commission will seek cooperation in the **G7 Cybersecurity Working Group**, to strengthen the cybersecurity of the health sector. In particular, the Working Group could consider possibilities to support the health sector against threats such as ransomware, building on reflections such as the Joint Statement on Ransomware Attacks Against Healthcare Facilities of 8 November 2024 presented in the context of the United Nations Security Council[46].

4. National Actions

The capacity of this Action Plan to improve cybersecurity in the health sector hinges on the active involvement and commitment of Member States. To successfully implement the Action Plan, Member States could designate **National Cybersecurity Support Centres specifically for hospitals and healthcare** providers. These centres would act as the primary points of contact for the health sector at national level, collaborating closely with the ENISA Support Centre. Where possible and relevant, Member States should designate existing bodies, such as national health CSIRTs or relevant authorities, as National Cybersecurity Support Centres.

Member States are also encouraged to create **national action plans focused on cybersecurity in the health sector**. These plans would outline the specific cybersecurity risks faced by healthcare systems and the national actions being taken to address them, while also ensuring that European-level resources and practices are effectively used. The ENISA Support Centre can assist in developing these plans, taking into account already existing national plans and coordinating efforts to ensure that the resources and strategies of individual Member States complement each other.

Another key focus for Member States is facilitating resource sharing among healthcare providers, which could be achieved through **joint procurement or pooled resources** at the national, regional, or even

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

European level. This approach would reduce the financial burden on individual entities while increasing their bargaining power with cybersecurity service providers.

For example, the French CaRE programme[47] has introduced a number of measures at national and regional level to address challenges in resourcing: a cyber catalogue provides an overview of cyber solutions and packages made available to hospitals through the national cybersecurity agency, the digital health agency, regional agencies, national purchasing organisations as well as commercial solutions. This is complemented by additional funding for regional agencies to offer shared resources.

Member States should also address the insufficient levels of investment in cybersecurity within the health sector. To ensure adequate funding, they should set **non-binding benchmarks and monitor funding targets aimed specifically at cybersecurity**, while ensuring that these investments do not detract from essential patient care. These funding targets should also aim to integrate security considerations into all digital investments in the sector. Member States can exchange best practices and advice on these targets through platforms such as the eHealth Network[48].

5. Public-Private Cooperation

Public-private cooperation and consultation with healthcare providers, other health sector entities, as well as relevant cybersecurity industry players, is essential for the successful implementation of the Action Plan. To further feed into the work of the Support Centre, the **Commission, supported by ENISA, will set up a joint Health Cybersecurity Advisory Board** with high-level representatives of both fields, healthcare and cybersecurity, which can advise the Commission and the Support Centre on impactful actions and discuss the further development of public-private partnerships in this field. The board will build on existing efforts for public-private partnerships, including the European Health ISAC.

Furthermore, the Commission will launch **a call for action** for cybersecurity companies, foundations, educational institutions, and industry stakeholders **to pledge actions to address the challenges in the sector**. Building on the experience of the Cybersecurity Skills Academy, such commitments could be for instance pledges under the Cybersecurity Skills Academy to include the provision of training courses and materials with a focus on health sector for cybersecurity professionals[49]. Other commitments could also address awareness raising activities or the provision of managed security services to specifically vulnerable entities for free or at reduced cost in order to increase their preparedness and cybersecurity resilience. Moreover, the commitments could consist in sharing cyber threat intelligence with the ENISA Support Centre. The Support Centre should maintain an overview of pledges made under the call for action, with the goal of ensuring their coherence and complementarity.

[47] French Digital Health Agency: Cybersécurité acceleration et Résilience des Établissements (CaRE). Available at https://esante.gouv.fr/strategie-nationale/cybersecurite.
[48] The eHealth Network is a voluntary network of national authorities responsible for eHealth designated by the Member States and established under Article 14 of Directive 2011/24/EU.
[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform

6. Deterring cyber threat actors

The EU's internal and external cybersecurity policies should support the goal of deterring cyber threat actors from attacking European healthcare systems. Cyberattacks against healthcare organisations are a particularly unacceptable type of malicious cyber activity, given their capability to threaten patient safety and human lives. Therefore, the full force of the EU's deterrence capabilities in the field of cybersecurity and law enforcement should be used to undermine the overall business model of threat actors targeting the health sector, and to deprive them of easy profits. This would include fostering cross-border investigations through enhanced sharing of indicators of compromise and other relevant data, and an increased focus on high-value targets and key criminal facilitators such as bulletproof hosting or crypto-currency mixing services.

The **Cyber Diplomacy Toolbox** offers a framework to prevent, deter and respond to cyberattacks against the EU, Member States and partners. The High Representative will continue to use the existing cyber sanctions framework to respond to threats targeting health systems.

Holding criminal actors accountable for their actions is an important deterrent. Therefore, Member States should ensure that law enforcement is fully integrated into their national action plans. In particular, they should make full use of the provisions under the Directive on attacks against information systems[50] and under the Council of Europe's Budapest Convention on Cybercrime to deter attacks, bring criminals to justice and to dismantle criminal infrastructures facilitating attacks[51]. Successful implementation of these tools should ensure that criminal and malicious actions against healthcare are punished.

7. Implementing and monitoring the Action Plan

Throughout this Action Plan, a number of tasks have been foreseen for a Support Centre to be established within ENISA. This ensures a holistic and coherent implementation of the Action Plan while avoiding the creation of new entities leading to potential overlaps and overhead costs. The Commission intends to ensure the appropriate resourcing of the Support Centre.

Once the Support Centre is operational, ENISA, in consultation with the Commission, should regularly provide updates of the Support Centre's work to the ENISA Management Board as well as relevant networks of Member States, in particular the NIS Cooperation Group, CSIRTs Network, the eHealth Network and where relevant, the European Health Data Space Board. Furthermore, ENISA should continually exchange with the public-private Health Cybersecurity Advisory Board about the implementation of actions provided by the Support Centre.

ENISA's regular reports, such as the Report on the State of Cybersecurity in the Union, which provides an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the EU, including in the health sector, should serve as occasions to publish relevant data, supporting the

[50] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng
[51] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols: https://www.coe.int/en/web/cybercrime/the-budapest-convention

monitoring of the Action Plan. Furthermore, ENISA's EU Cybersecurity Index[52] can provide quantitative and qualitative data, serving as an evidence base for assessing the criticality and maturity of the health sector.

8. Next steps

This Communication has set out an ambitious agenda for a more cybersecure health sector in the EU. With the proposed development of the Cybersecurity Support Centre for Hospitals and Healthcare Providers at the heart of ENISA, the Action Plan sets out an avenue towards the creation of a coherent and shared European approach to the challenge of cybersecurity in the sector.

This Communication should be seen as the start of a process to improve cybersecurity in the health sector. Therefore, the adoption of the Action Plan will be accompanied by the launch of comprehensive stakeholder consultations and the continuation of exchanges with Member States and relevant networks to collect insights. Based on the results of the consultations, the Commission intends to come forward with recommendations in the fourth quarter of 2025 to further refine the Action Plan.

The Commission calls on Member States and all stakeholders to work together in delivering on the ambition of the Action Plan.

[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note (2024). Available at https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ANNEX – Overview of proposed actions

The Commission:

ENISA Cybersecurity Support Centre for Hospitals and Healthcare Providers	
Ensure appropriate resources for the Cybersecurity Support Centre Work with the ECCC to launch pilot projects to develop best practices for cyber hygiene and security risk assessment, and to address the need for continuous cybersecurity monitoring, threat intelligence and incident response using state-of- the art cybersecurity solutions, for the development of the European Cybersecurity Support Centre's service catalogue	2025
Preventing cybersecurity incidents	
In consultation with the NIS Cooperation Group, EU-CyCLONe and ENISA, explore identifying health as a sector for which support can be given for coordinated preparedness testing under the Cyber Solidarity Act	Q1 2025
Rapid Response and Recovery	
Together with ENISA, ensure the EU Cybersecurity Reserve includes a Rapid Response Service specifically for the health sector	Q4 2025
Public-Private Cooperation	
Supported by ENISA, set up a joint Health Cybersecurity Advisory Board	Q1 2025
Launch a call for action for cybersecurity companies, foundations, educational institutions, and industry stakeholders to pledge actions to address the challenges in the health sector	Q2 2025
Deterring cyber threat actors	
Together with the High Representative, explore the use of Cyber Diplomacy Toolbox measures to prevent, discourage, deter and respond to malicious activities against health systems	2025
Advance international cooperation against ransomware actors, notably in the International	2025-2026

Counter Ransomware Initiative, working together with the High Representative	
Seek cooperation in the G7 Cybersecurity Working Group to strengthen the cybersecurity of the health sector	2025-2026
Next steps	
Launch comprehensive stakeholder consultations	Q1 2025
Adopt recommendations to further refine the Action Plan	Q4 2025

ENISA:

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers	
Begin work to establish a European Cybersecurity Support Centre for hospitals and healthcare providers	Q2 2025
Develop a comprehensive service catalogue to be provided by the Cybersecurity Support Centre	From Q4 2025
Preventing cybersecurity incidents	
Issue guidance that highlights the most critical cybersecurity practices and aid healthcare providers in implementing them	Q3 2025
In close collaboration with Commission and Member States, develop a regulatory mapping tool	Q1 2025
Develop a framework for cybersecurity maturity assessments specific to healthcare	Q3 2025
Carry out an annual Health Cyber Maturity Assessment	2025-2026
Collaborate with Member States and regional programme authorities to create Cybersecurity Voucher model programmes	2025-2026
Develop new procurement guidelines for cybersecurity of hospitals and healthcare providers	Q3 2025
Create a European Health CISOs Network	Q1 2026

Design and promote training modules and courses for healthcare professionals	Q1 2026
European capabilities for detecting cyber threats against the health sector	
Build up a European KEV catalogue for medical devices, electronic health record systems and providers of ICT equipment and software in health	Q4 2025
Introduce an EU-wide early warning subscription service for the health sector	As of 2026
Support the European Health ISAC with tools and information exchange	2025-2026
Rapid Response and Recovery	
Together with the Commission, ensure the EU Cybersecurity Reserve includes a Rapid Response Service specifically for the health sector	Q4 2025
In collaboration with the CSIRTs Network, develop cyber incident response playbooks tailored for healthcare	Q3 2025
Facilitate a large roll out of national cybersecurity exercises to test the playbooks and strengthen incident response protocols	As of Q4 2025
Provide a ransomware recovery subscription service	As of 2026
Together with Europol, identify the most common ransomware strains targeting healthcare organisations and expand the repository of decryption tools through the No More Ransom project.	Q4 2025
Together with Europol, develop accessible guidance to help healthcare providers avoid paying ransoms	Q3 2025
National Actions	
Assist Member States in developing national action plans	2025
Coordinate efforts to ensure that resources and strategies of individual Member States complement each other	2025-2026
Implementing and monitoring the Action Plan	

In consultation with the Commission, regularly provide updates of the work of the Cybersecurity Support Centre to relevant networks of Member States	2025-2026
Continually exchange with the Health Cybersecurity Advisory Board	2025-2026

Member States:

European capabilities for detecting cyber threats against the health sector	
Share incident notifications from hospitals and healthcare providers under NIS2 with the European Cybersecurity Support Centre	As of Q4 2025
Encourage the development of national health ISACs	2025-2026
Preventing cybersecurity incidents	
Within the NIS Cooperation Group, perform a coordinated security risk assessment, assessing both technical and strategic risks related to medical devices supply chains	Q4 2025
Rapid Response and Recovery	
Roll out national cybersecurity exercises to test the playbooks and strengthen incident response protocols	As of 2026
National Actions	
Designate National Cybersecurity Support Centres for hospitals and healthcare providers	Q2 2025
Create national action plans focused on cybersecurity in the health sector	Q4 2025
Facilitate resource sharing among healthcare providers	2025-2026
Set non-binding benchmarks and monitor funding targets aimed specifically at cybersecurity	Q4 2025
Request healthcare organisations and other entities subject to the NIS2 Directive to report their intentions to pay ransoms	Q4 2025