

Targeted consultation – Action Plan on the cybersecurity of hospitals and healthcare providers

Fields marked with * are mandatory.

Introduction

On 15 January 2025, the European Commission adopted an Action Plan on the cybersecurity of hospitals and healthcare providers. This consultation follows up on the Action Plan, with a view to gathering more information that can support the implementation and further refining of the planned actions.

For the purpose of this survey, we use the term ‘healthcare providers’ to refer to entities legally providing healthcare on the territory of a Member State. This can include hospitals, as well as other healthcare providers (e.g. offices of General Practitioners). Furthermore, the questionnaire offers the opportunity to provide inputs regarding other types of entities in the health sector (e.g. manufacturers of medical devices).

The cybersecurity threat landscape evolves continuously, reflecting geopolitical tensions, criminal opportunism and the vulnerabilities and risks which accompany rapid digitalisation of the healthcare sector’s critical infrastructure and services. The actions defined in the Action Plan aim to strengthen the cybersecurity maturity of the healthcare sector, and the ability of the EU cybersecurity ecosystem to support healthcare entities in preventing, deterring, detecting and responding to cyber threats.

This survey is targeted at a wide variety of stakeholders, such as healthcare IT professionals, managers in hospitals and healthcare providers, healthcare professionals, healthcare authorities, patients, compliance and data privacy professionals, cybersecurity and healthcare industry, and academia. Some of the questions in the survey are optional. The multiple-choice questions take approximately 15 minutes to complete. Additionally, you may add further written inputs.

Who should respond to this questionnaire?

All respondents are welcome to answer the survey. In particular, the Commission welcomes responses from:

- Managerial staff of hospitals and healthcare providers
- Healthcare IT professionals
- Healthcare professionals
- Healthcare authorities
- Patients, and organisations representing patients
- Compliance and data privacy professionals
- Cybersecurity industry players

- Healthcare industry players

About you

* First name

Sara

* Surname

Roda

* Email (this won't be published)

sara.roda@cpme.eu

* Country of origin

- AT - Austria
- BE - Belgium
- BG - Bulgaria
- HR - Croatia
- CY - Cyprus
- CZ - Czechia
- DK - Denmark
- EE - Estonia
- FI - Finland
- FR - France
- DE - Germany
- EL - Greece
- HU - Hungary
- IE - Ireland
- IT - Italy
- LV - Latvia
- LT - Lithuania
- LU - Luxembourg
- MT - Malta
- NL - Netherlands
- PL - Poland
- PT - Portugal
- RO - Romania
- SK - Slovak Republic
- SI - Slovenia
- ES - Spain
- SE - Sweden
- Non-EU - Other

* I am giving my contribution as

- Representing myself
- Representing the organisation that I work for
- Representing multiple organisations

Which organisation(s) do you represent?

200 character(s) maximum

CPME - Standing Committee of European Doctors - AISBL

* In what areas of activity are you involved? (Choose all that apply)

"Provision of compliance and data privacy protection services": For example, company that helps hospitals or healthcare providers to be compliant with data protection rules

"Provision of cybersecurity insurance": For more information about cyber insurance, see https://www.eiopa.europa.eu/browse/digitalisation-and-financial-innovation/cyber-insurance_en

- Provision of healthcare services (hospitals and healthcare providers)
- Provision of cybersecurity services for healthcare organisations
- Provision of compliance and data privacy protection services
- Advocacy (e.g. patient organisations, NGOs, health professional representatives)
- Patient
- Regulatory authority
- Provision of cybersecurity insurance

Please provide any further information about you or your organisation that is relevant in the context of this consultation

500 character(s) maximum

represents national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues.

Key challenges

* What is your perception of the current overall level of cybersecurity maturity of the healthcare sector in your country?

- Very advanced
- Advanced
- Medium
- Basic
- Weak
- I don't know / I am not in a position to assess it

In your opinion, what are the most important challenges to ensure cybersecurity of hospitals? (Rank each option on a scale of 1 – 10: "Not important" – "Very important")

"Availability and use of cybersecurity tools": For example software tools used for managing cybersecurity risks, or monitoring cyber threats

"Cybersecurity in the supply chain": In this context, cybersecurity in the supply chain is understood as the cybersecurity-related aspects concerning the relationships between a healthcare organisation on the one hand, and its suppliers and service providers on the other hand

	1	2	3	4	5	6	7	8	9	10
Cybersecurity skills of responsible cybersecurity professionals in hospitals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cybersecurity awareness of healthcare professionals and other non-IT professionals in hospitals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Presence of effective cybersecurity processes and governance structures in hospitals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Availability and use of cybersecurity tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Availability of cybersecurity services and/or support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cybersecurity in the supply chain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Detection of cybersecurity threats	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Receiving timely information about cybersecurity threats	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ability to respond to and recover from cybersecurity threats and incidents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

In your opinion, what are the most important challenges to ensure cybersecurity of healthcare providers other than hospitals? (Rank each option on a scale of 1 – 10: “Not important” – “Very important”)

"Availability and use of cybersecurity tools": For example software tools used for managing cybersecurity risks, or monitoring cyber threats

"Cybersecurity in the supply chain": In this context, cybersecurity in the supply chain is understood as the cybersecurity-related aspects concerning the relationships between a healthcare organisation on the one hand, and its suppliers and service providers on the other hand

	1	2	3	4	5	6	7	8	9	10
Cybersecurity skills of responsible cybersecurity professionals of the healthcare providers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cybersecurity awareness of healthcare professionals and other non-IT professionals in the healthcare providers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Presence of effective cybersecurity processes and governance structures of the healthcare providers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Availability and use of cybersecurity tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Availability of cybersecurity services and/or support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cybersecurity in the supply chain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Detection of cybersecurity threats	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Receiving timely information about cybersecurity threats	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ability to respond to and recover from cybersecurity threats and incidents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

In your perception, do you think that healthcare entities in your country dedicate enough spending on ICT in general?

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

In your perception, do you think that healthcare entities in your country dedicate enough investments to cybersecurity, as a part of their overall ICT spending?

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

Do you think that your organisation is dedicating enough investments to cybersecurity, as part of its overall ICT spending?

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know / I am not in a position to assess it

The following questions elaborate on specific types of challenges.

Questions on the capacities of hospitals and healthcare providers

Supply chain security: In your opinion, what are the most important cybersecurity challenges for hospitals and healthcare providers when using products and services originating from third parties? (Rank the options on a scale of 1 – 10: “Not important” to “Very important”)

"Difficulty to keep up with the necessary security updates": For example software updates that address security vulnerabilities in the product

	1	2	3	4	5	6	7	8	9	10
Lack of funding and resources for hospitals and healthcare providers to select secure suppliers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of awareness regarding supply chain cybersecurity risks among hospitals and healthcare providers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Difficulty in ensuring diversity of suppliers, or limited availability of suppliers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Difficulty of ensuring that suppliers follow good cybersecurity practices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Difficulty to keep up with the necessary security updates	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

In your opinion, what are the most important challenges for the **detection** of cybersecurity threats in hospitals? (Rank the options on a scale of 1 – 10: “Not important” to “Very important”)

	1	2	3	4	5	6	7	8	9	10
Lack of funding and resources for hospitals (e.g. human resources, tools)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of timely information about cybersecurity threats received from authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of information-sharing about cybersecurity threats with players in the cybersecurity and healthcare ecosystems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lack of detection tools, techniques, and protocols, or awareness about them	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Lack of qualified cybersecurity professionals to detect or follow up on information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lack of knowledge among healthcare professionals on how to detect and report suspicious events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

In your opinion, what are the most important challenges for the **detection** of cybersecurity threats in healthcare providers organisations other than hospitals? (Rank the options on a scale of 1 – 10: “Not important” to “Very important”)

	1	2	3	4	5	6	7	8	9	10
Lack of funding and resources for healthcare providers (e.g. human resources, tools)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of timely information about cybersecurity threats received from authorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of information-sharing about cybersecurity threats with players in the cybersecurity and healthcare ecosystems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of detection tools, techniques, and protocols, or awareness about them	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of qualified cybersecurity professionals to detect or follow up on information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lack of knowledge among healthcare professionals on how to detect and report suspicious events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

In your opinion, what are the most important challenges for the ability of **hospitals to respond to and recover from cybersecurity incidents**? (Rank the options on a scale of 1 – 10: “Not important” to “Very important”)

	1	2	3	4	5	6	7	8	9	10
Lack of funding and resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of cybersecurity professionals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of training for relevant staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lack of established procedures for business continuity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Lack of established procedures for incident response	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of information about available support mechanisms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of available support mechanisms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Available support services do not have competence for addressing specific healthcare sector challenges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Difficulties in interactions with suppliers (e.g. supplier of a product from which a cybersecurity incident originates)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

In your opinion, what are the most important challenges for the ability of **healthcare providers** (other than hospitals) to **respond to and recover from cybersecurity incidents**? (Rank the options on a scale of 1 – 10: “Not important” to “Very important”)

	1	2	3	4	5	6	7	8	9	10
Lack of funding and resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of cybersecurity professionals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of training for relevant staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of established procedures for business continuity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of established procedures for incident response	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of information about available support mechanisms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Lack of available support mechanisms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Available support services do not have competence for addressing specific healthcare sector challenges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Difficulties in interactions with suppliers (e.g. supplier of a product from which a cybersecurity incident originates)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

In your opinion, what are the most effective actions that hospitals and healthcare providers can take against cybersecurity threats? (Rank each option on a scale of 1 – 10: “Not important” to “Very important”)

	1	2	3	4	5	6	7	8	9	10

Ensuring adequate financial and human resources for cybersecurity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Establishing internal procedures for cybersecurity management (e.g. risk analysis, incident handling, business continuity)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Establishing internal procedures for cybersecurity of the organisation's ICT supply chain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Providing cyber awareness training to staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Continuously assessing the effectiveness of cybersecurity risk management measures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cooperating with other hospitals and healthcare providers (e.g. through cybersecurity information-sharing initiatives)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperating with public authorities, national Computer Security Incident Response Teams or other players in the cybersecurity ecosystem (e.g. using resources made available by authorities)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Obtaining services from cybersecurity service providers (e.g. Managed Security Service Providers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

In your opinion, which of the following actions are currently **not sufficiently** taken by hospitals and healthcare providers? Please rank the options in order of importance, giving the highest ranking to measures that must be improved the most.

	1	2	3	4	5	6	7	8	9	10
Ensuring adequate financial and human resources for cybersecurity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Establishing internal procedures for cybersecurity management (e.g. risk analysis, incident handling, business continuity)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Establishing internal procedures for cybersecurity of the organisation's ICT supply chain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Providing cyber awareness training to staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Continuously assessing the effectiveness of cybersecurity risk management measures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperating with other hospitals and healthcare providers (e.g. through cybersecurity information-sharing initiatives)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cooperating with public authorities, national Computer Security Incident Response Teams or other players in the cybersecurity ecosystem (e.g. using resources made available by authorities)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Obtaining services from cybersecurity service providers (e.g. Managed Security Service Providers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Preventing cybersecurity incidents

The Action Plan envisages that a Support Centre for cybersecurity of hospitals and healthcare providers, to be established within the EU Agency for Cybersecurity (ENISA), will develop a catalogue of services supporting preparedness, prevention, detection and response.

What services should the Support Centre offer to improve cybersecurity of hospitals and healthcare providers? You may describe elements highlighted in the Action Plan, as well as other elements.

1000 character(s) maximum

The service catalogue is further described on page 7 of the Action Plan: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0010>

Vehicle to apply for cybersecurity voucher programme – all MS include a reference to entity providing the voucher at national level & applications made via the Support Centre; Providing best practices & a catalogue with security measures for HC providers on cybersecurity; Providing free online awareness raising, training modules & courses; Provide catalogue with trustworthy & secure cybersecurity software solutions, such as risk assessment tools, decryption tools to avoid paying ransoms, real-time detection systems, privacy-preserving data-sharing platforms; Provide latest information on cyberthreats & how to be protected; Permanent support center for monitoring different actors on the market & providing services combatting organised crime for the healthcare service; Emergency response teams to be set up in ENISA to complement the national emergency response teams; At the request of the HC provider and hospital, run tests, for free, to reveal how prepared/vulnerable IT infrastructure is.

Electronic identification (eID): What do you see as key challenges in access to computers and software in hospitals and other healthcare providers? (Choose all that apply)

- Use and management of passwords for different software
- Computers left unlocked
- Shared use of computers

- Handling of access rights (e.g. difficulty to access required systems, or overly wide access that leads to increased risks)
- Unavailability of alternative login methods when the usual method (e.g. smart card) is not accessible (for example forgotten at home)
- Other (Please elaborate below)

Please elaborate:

200 character(s) maximum

EHR use,identification&authentication processes must be secure.Protective equipment of HCP while practicing needs to be considered;Need for usable&secure ways of authentication, other than passwords.

As a part of the Action Plan, 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 national and EU levels.

Preparedness and targeted support: What aspects should be analysed by the annual Health Cyber Maturity Assessment?

- Level of implementation of specific cybersecurity measures in the healthcare sector
- Level of investment in cybersecurity in the healthcare sector
- Level of cybersecurity awareness among healthcare staff
- Overview of cyber threats and incidents relevant for the healthcare sector
- National-level assessments about cybersecurity maturity in the healthcare sector
- Other (Please elaborate below)

As a part of the Action Plan, Member States should consider targeted measures like Cybersecurity Vouchers for micro, small and medium-sized hospitals and healthcare providers. These vouchers would provide financial assistance to put in place specific cybersecurity measures.

Preparedness and targeted support: What would be the most effective method for introducing the Cybersecurity Vouchers?

- Member States develop the conditions for distributing the Vouchers based on the relevant national context
- The EU Cybersecurity Agency (ENISA) proposes common European-wide conditions for distributing the Vouchers, which Member States can adapt
- The European Cybersecurity Competence Centre (ECCC) distributes funding via the National Competence Centres
- I don't know / No response
- Other (Please elaborate below)

Preparedness and targeted support: What types of measures should the Cybersecurity Vouchers support as a priority? (Choose all that apply)

- Supporting the development and implementation of policies on risk analysis and information system security
- Supporting the development and implementation of cybersecurity incident handling methods
- Supporting the development and implementation of business continuity and crisis management plans
- Enhancing supply chain cybersecurity
- Supporting cybersecurity in the acquisition, development and maintenance of network and information systems (e.g. vulnerability handling)

- Supporting the development and implementation of policies and procedures to assess effectiveness of cyber risk-management measures
- Supporting basic cyber hygiene practices and cybersecurity training
- Supporting the development and implementation of policies on the use of cryptography
- Supporting the development and implementation of policies on human resources security, access control and asset management
- Supporting the use of secure authentication solutions
- Other (Please elaborate below)

The Medical Devices Regulation and the Regulation on in-vitro diagnostic medical devices set requirements for cybersecurity of these devices in the internal market.

Cybersecurity in healthcare supply chains: Besides the applicable rules for medical device cybersecurity and post-market surveillance requirements, to what extent would the following measures be beneficial for connected medical devices? (Rank each option on a scale of 1 – 10: “Not beneficial” – “Very beneficial”)

"Standards or common specifications": Under the conditions described in Articles 8–9 of the Medical Devices Regulation and of the Regulation on in-vitro diagnostic medical devices, devices that conform with harmonised standards are presumed to comply with the Regulations. Where harmonised standards do not exist or are not sufficient, the Commission may adopt common specifications. In that case, devices that conform with the common specifications are presumed to comply with the Regulations.

	1	2	3	4	5	6	7	8	9	10
Foster an efficient flow of information on cybersecure use of medical devices for hospitals and healthcare providers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Prioritising cybersecurity requirements of connected medical devices in procurement practice	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Introduce targeted notification requirements for hospitals or healthcare provider incident response planning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Strengthen implementation of cybersecurity requirements within the current regulatory framework (e.g. standards or common specifications)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Securing healthcare supply chains: What actions should the EU take to ensure cybersecurity of cloud solutions used in the healthcare sector?

- Targeted guidance for hospitals and healthcare providers on cybersecure use of cloud solutions
- Targeted guidance for cloud service providers on the implementation of baseline security measures
- Targeted guidance for hospitals and healthcare providers on procurement of cloud solutions
- Voluntary EU-level cybersecurity certification for cloud services
- Other (Please elaborate below)

Please elaborate:

200 character(s) maximum

Stimulate the development of EU cloud systems.

The Action Plan envisages the creation of a European Health CISOs Network, bringing together Chief Information Security Officers (CISOs) working for healthcare organisations.

Training and skills development: What actions should the European Health CISOs Network undertake in order to facilitate exchanges among cybersecurity professionals in the health sector?

"Cybersecurity role profiles": The EU Cybersecurity Agency ENISA has created a European Cybersecurity Skills Framework, which defines a set of 12 typical cybersecurity professional role profiles: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>

- Regular conferences and training sessions for members of the Network
- Facilitate sharing of best practices and guidance (e.g. through a dedicated webpage or portal)
- Create a mentoring scheme which pairs CISOs together
- Coordinate an assessment of the cybersecurity role profiles needed by hospitals and healthcare providers
- Development of joint policy papers about relevant issues
- Other (Please elaborate below)

Training and skills development: How should synergies be ensured between the European Health CISOs Network, and the European Health ISAC?

The European Health ISAC (Information Sharing & Analysis Centre) brings together healthcare stakeholders in a trusted community for collecting, analysing and disseminating cybersecurity threat information among its members.

- Joint meetings between the networks
- Inviting members of one network to also join as members of the other network (mutual membership)
- Involving the European Health ISAC in specific tasks of the European Health CISOs Network
- Other (Please elaborate below)

Training and skills development: Which topics should be addressed by cybersecurity training modules for healthcare professionals (e.g. doctors or nurses)?

- Secure practices in the use of healthcare-related software
- Secure practices in the use of medical devices
- Secure practices in the use of general purpose software and devices
- Training on established procedures in case of an incident
- General awareness of the most common cybersecurity threats
- Other (Please elaborate below)

Please elaborate:

200 character(s) maximum

Training tailored to healthcare professionals' practice.

Cybersecurity insurance: What actions should the EU take to maximise the benefits of cybersecurity insurance schemes for the cyber resilience of hospitals and healthcare providers?

- Organising discussions between cyber insurance providers and healthcare providers on the specific challenges of the healthcare sector

- Preparation of model contractual clauses for cyber insurance schemes
- Restrictions against cyber insurance schemes that cover for ransom payments made to perpetrators of ransomware attacks
- No actions are needed
- Other (Please elaborate below)

The [European Health Data Space \(EHDS\)](#) Regulation aims to establish a common framework for the use and exchange of electronic health data across the EU.

EHDS: In what ways can implementation of the Action Plan contribute to a secure European Health Data Space (EHDS)? Please indicate the 3 most important cybersecurity actions to support the EHDS and the secure exchange of health data.

1000 character(s) maximum

- Essential technical features for robust cybersecurity should be implemented from design and by default into EHR systems and cloud services by healthcare software industry;
- Ensure secure channels to exchange health data between patients to healthcare professionals (HCP) and vice-versa; HCP to HCP; HCP to Health Data Access Bodies/ national competent authorities
- If the implementation of action plan leads to better end point security, this will lead to a more robust and resilient EHDS infrastructure. The high level of security needs to be accompanied by high level of usability.

European capabilities for detecting cyber threats against the health sector

As a part of the Action Plan, the Support Centre should introduce an EU-wide early warning subscription service for the health sector, delivering near-real-time alerts about cyber threats. Organisations do not need to pay a subscription fee to benefit from the subscription service.

What kind of information should an EU-wide early warning subscription service provide to hospitals and healthcare providers?

- Information about ongoing relevant cybersecurity incidents
- Information about tactics, techniques and procedures (TTPs) of cyber threat actors
- Information about vulnerabilities in ICT products
- Other (Please elaborate below)

Rapid response and recovery

The EU Cybersecurity Reserve provides incident response services from trusted private providers, to assist with significant or large-scale cybersecurity incidents and initial recovery efforts. The EU Cybersecurity Reserve should include a Rapid Response Service specifically for the health sector.

What services should be prioritised for the health sector as a part of the Rapid Response Service? (Choose all that apply)

"Information Security Incident Analysis": Triage – prioritisation and categorisation, information collection, detailed analysis coordination, information security incident root cause analysis, cross-incident correlation, immediate recovery – these services help organisations understand the attack vectors and assist them with technical response capabilities and handling incidents effectively

"Artefact and Forensic Evidence Analysis": Malware forensics and network forensics – these are specific services needed for a more extensive and complex response process

"Information Security Incident Coordination": Communication between involved parties, notification distribution to constituents, activities coordination, incident reporting to relevant authorities, media communication – these services constitute the crisis-management pillar of the incident handling, which can include guidance on the strategic level

- Support Information Security Incident Analysis
- Support Artefact and Forensic Evidence Analysis
- Support Information Security Incident Coordination
- I don't know / I don't wish to respond
- Other (Please elaborate below)

The Action Plan envisages the creation of a ransomware recovery subscription service, which supports hospitals' and healthcare providers' effective recovery against ransomware attacks. Organisations do not need to pay a subscription fee to benefit from the subscription service.

What kind of support should an EU-wide ransomware recovery subscription service provide for hospitals and healthcare providers?

- Guidance on the preparation of recovery plans
- Guidance on the use of available tools against ransomware, e.g. decryption tools
- Guidance on how to avoid paying ransom in the case of a ransomware incident
- Training courses on how to recover from ransomware attacks
- Enlarging the repository of available tools against ransomware, e.g. decryption tools
- Other (Please elaborate below)

National actions & Public-private cooperation

Member States are encouraged to create national action plans focused on cybersecurity in the health sector. 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.

What elements would you like to be addressed in national action plans on cybersecurity in the health sector?

- Priority actions to increase the cyber resilience of the sector in the Member State
- Assessment of cybersecurity risks facing healthcare system(s) in the Member State
- Actions to ensure that available European-level resources are easily accessible to hospitals and healthcare providers
- Simulation exercises and trainings at national and/or local level
- Cybersecurity awareness training for healthcare professionals
- Benchmarks and funding targets related to cybersecurity in healthcare organisations
- Other (Please elaborate below)

The Commission will launch a Health Cybersecurity Advisory Board with representatives from the healthcare and cybersecurity fields. The Advisory Board can provide its views on impactful actions for cybersecurity in the sector, and discuss the further development of public-private partnerships.

What actions should the Health Cybersecurity Advisory Board undertake in order to provide advice on cybersecurity in the sector?

- Development of joint policy papers about relevant issues
- Identification of best practices to be shared
- Disseminating information to hospitals and healthcare providers
- Other (Please elaborate below)

Conclusion

Please elaborate on your views regarding actions required at the EU level in support of cybersecurity of hospitals and healthcare providers. You may indicate which types of actions bring the most added value when taken at EU level, and which actions bring the most added value when taken at national or regional level.

1000 character(s) maximum

CPME welcomes the Action Plan proposed by the European Commission. The actions with most added EU value relate to financing and the catering of services that the European Cybersecurity Support Centre in ENISA could offer (please see response to question on which services should the support Centre offer). The EU should continue to raise awareness among Member States to ensure that cybersecurity is considered to be a matter of national public security and stimulate European cloud service providers. The Commission should encourage the availability of managed security cloud services for the healthcare sector. Financial investment needs to be permanent, not only for implementation but also sustainability (upgrades, expertise sharing, cybersecurity standards, open source AI-driven solutions). At national level, provide clear guidance and find appropriate channels to inform local practices of new available trustworthy cybersecurity solutions.

Please elaborate on your views regarding actions at national/regional level. What actions would be necessary that are not addressed or only partly addressed today?

1000 character(s) maximum

Ensure proper contingency plans in case of a general blackout, for example introduce mandatory functioning of independent generators in hospitals.
Develop technology with high level of security and at the same time a high level of usability and reliability.

Is there anything else you would like to share?

1000 character(s) maximum

Methods for identification & authentication of HCP & patients in online EHR systems need to be robust, easy, fast & with appropriate levels of security to protect personal data relevant for clinical activities in compliance with eIDAS Regulations. Identification & authentication of doctors in online EHR systems should balance the need for integrity in a certain setting & the security of the digital tool with the admin burden for this procedure. Protective equipment HCPs use while practicing needs to be considered. CPME supports SSO authentication & identity management federation concepts. 'One day, one-time login' to the online EHR

system back-end should be common practice, providing for automatic authentication of national components, such as ePrescriptions, PS, etc. This means that the session should remain active until the HCP signs out, which does not invalidate the authentication procedure of locking &unlocking the system when a HPC is required to use another terminal on the same day.

You may upload an attachment below:

Only files of the type pdf,doc,docx,odt,txt,rtf are allowed

b5ccafba-44bf-4f8f-9854-9c194f0d352f/cpme_ad_22032025_015.final.policy.implementing.user-friendly.ehds.pdf

Contact

EC-HEALTHCARE-CYBERSECURITY@ec.europa.eu