EAEP POSITION PAPER ON THE EUROPEAN ACTION PLAN ON THE CYBERSECURITY OF HOSPITALS AND HEALTHCARE PROVIDERS

The **European Association of E-Pharmacies (EAEP)** welcomes the publication by the European Commission of the **European Action Plan on the cybersecurity of hospitals and healthcare providers**. Healthcare providers, including hospitals, clinics, and pharmacies, are increasingly reliant on digital technologies to deliver care, manage patient records, and provide essential services. As key stakeholders in the healthcare ecosystem, online pharmacies recognise the critical importance of safeguarding health data, systems, and services against the increasing threat of cyberattacks. This is essential not only for patient safety and privacy but also for maintaining trust in the healthcare system at large.

The EAEP fully shares the main objective of the Action Plan, namely to increase the cybersecurity of assets of healthcare facilities, especially information systems and information contained therein, using appropriate functions, processes, services, and tools consisting of software, hardware and quality security documentation. Particularly in view of the significant increase in threats such as ransomware and data leaks in recent years, action to protect sensitive infrastructure is urgently needed. Recognising the international scope of healthcare threats, the EAEP advocates for collaboration with non-EU partners to align and secure broader European cybersecurity standards effectively.

RECOMMENDATIONS

With a view to contributing to the implementation of the Action Plan and making it future-proof and fit-for-purpose, herewith, the EAEP wishes to emphasise the **importance of reliable and safe pharmaceutical services**, highlighting the necessity for **robust cybersecurity measures in online pharmaceutical operations**.

Specifically, the following issues deserve urgent and dedicated action:

- **Fostering a resilient and user-oriented data protection framework**

  Protecting patients' health data and safeguarding their health is of crucial importance for pharmacies. In this sense, online pharmacies – as key actors along the supply chain handling sensitive patient data on a daily basis – implement safe and innovative processes to treat patients' health data as securely and responsibly as possible. Our members already take proactive and stringent measures with regard to data protection and cybersecurity which are implemented on a continuous basis. These measures are fundamental to providing a secure and safe digital health service, prioritising the safety and health of patients. As such, we **call on the European Commission to cover all healthcare providers, including pharmacies operating online, in the upcoming legislative and non-legislative initiatives listed in the Action Plan**. Digitalising pharmacy services requires robust cybersecurity measures beyond those in traditional healthcare settings. Future initiatives must therefore adopt a holistic, inclusive, and coordinated approach that addresses the **cybersecurity needs of the entire**

healthcare sector and secures the entire pharmaceutical supply chain, from prescription to delivery. All actors involved should meet high cybersecurity standards.

New measures should aim at protecting sensitive data while empowering healthcare providers as pharmacists to make use of patient's health data with a view to ensuring the best possible health outcome.

- **Capacity building, training & public awareness**

In addition to traditional hacker attacks, human error continues to be one of the greatest potential threats to cybersecurity nowadays. Regardless of the technological and safety measures in place, the human factor can still hamper and thus become a liability for successful prevention of cyber attacks. To address this shortcoming, comprehensive and **recurring training and further education becomes fundamental**. In this sense, the healthcare workforce should be equipped with a concrete set of actions to respond to an emergency, and learning content must always be up to date-and constantly adapted to new trends and threats. Due to the high costs associated with such training and education, **dedicated EU and national funding should be allocated** to ease the financial burden on healthcare providers. This would enable e-pharmacies, particularly small and medium-sized enterprises (SMEs), to afford the necessary tools, technologies, and expertise to safeguard their systems against cyber threats.

EAEP members' perspective

Data protection in practice: Avoiding human error

To ensure effective risk management, some EAEP members educate their employees on cybersecurity risks and how to avoid possible data breaches with targeted training to avoid human error. Employees/pharmacists are typically a classic target group for attacks such as phishing e-mails or social engineering. Through training and test runs, healthcare professionals are made aware of possible dangers and are pointed to potential attacks and the associated actions and instructions to follow in case of an emergency.

Nonetheless, **raising awareness among the broader public** remains an important aspect that the initiatives announced in the Action Plan must address in order to ensure that its mission is successfully achieved.

- **Investment in cybersecurity e-infrastructure and innovation**

  With a view to establishing effective and efficient protection in practice, substantial investments must be made in e-infrastructure. However, to maintain ongoing security, these investments cannot be one-time efforts; they must be continuous. Both **software and hardware require regular maintenance and upgrades** to meet security objectives in real-world scenarios. This will necessitate increased focus on research and development to address emerging threats, ensuring that infrastructure and the economy do not become vulnerable targets in the future. To identify key issues or potential risks, it is essential for authorities to **collaborate with not only traditional (analogue) stakeholders but also digital players in the healthcare sector**, such as e-pharmacies. It is crucial to engage actively with these stakeholders, listen to their concerns, and implement their requirements to address security challenges successfully.

- **Smooth and effective implementation**

  In addition to putting forward new measures to achieve the above-mentioned objectives, it is crucial to **clarify the role of the new initiatives proposed in the Action Plan within the existing broader legal framework**. The Action Plan should seamlessly align with related provisions, and its implementation must be coordinated with other ongoing initiatives or relevant laws in a practical and efficient manner. **Continuous dialogue with all stakeholders is essential to ensure the Action Plan's success**. In addition, cybersecurity is a shared responsibility between national governments, the EU, and private sector actors. E-pharmacies, which in some cases operate across borders, need a coherent and harmonised approach to cybersecurity. The implementation of the Action Plan should include provisions for integrating e-pharmacies into national and EU-level cybersecurity frameworks. This includes ensuring that e-pharmacies can participate in information-sharing initiatives, receive timely updates on emerging threats, and access resources that enable them to implement best practices in cybersecurity.

CONCLUSION

The EAEP fully supports the EU's initiative to strengthen cybersecurity in the healthcare sector. As the healthcare landscape continues to evolve with the increasing integration of digital technologies, it is imperative that the cybersecurity of e-pharmacies is addressed as part of the broader healthcare cybersecurity framework. The EU Action Plan on cybersecurity of hospitals and healthcare providers provides a timely opportunity to ensure that e-pharmacies, alongside hospitals and other healthcare providers, are equipped with the tools, resources, and regulations needed to safeguard patient safety and privacy in the digital age.

We urge the European Commission to take into account the specific needs of e-pharmacies in the implementation of the Action Plan, ensuring that all players in the healthcare ecosystem are equipped to face the growing cybersecurity challenges of the 21st century.

About EAEP:

The European Association of E-Pharmacies (EAEP) represents the voice of e-pharmacies on the European continent. The EAEP promotes its interests mainly with political stakeholders, regional and business actors, with the ultimate aim to improve the health of Europe's citizens and strengthen the European healthcare system. E-pharmacies have digitalised the classical pharmacy, and therefore act at the crossroads of digitalisation, healthcare, e-commerce and sustainability. As pioneers in digital healthcare, EAEP members innovate secure processes for managing health data, delivering medications, and providing digital healthcare services. Compliant with both national and EU regulations, all members are committed to advancing the quality, safety and efficiency of healthcare for all Europeans.

For more information, please contact:

Martino Canonico

Head of Brussels Office

martino.canonico@eaep.com