ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern
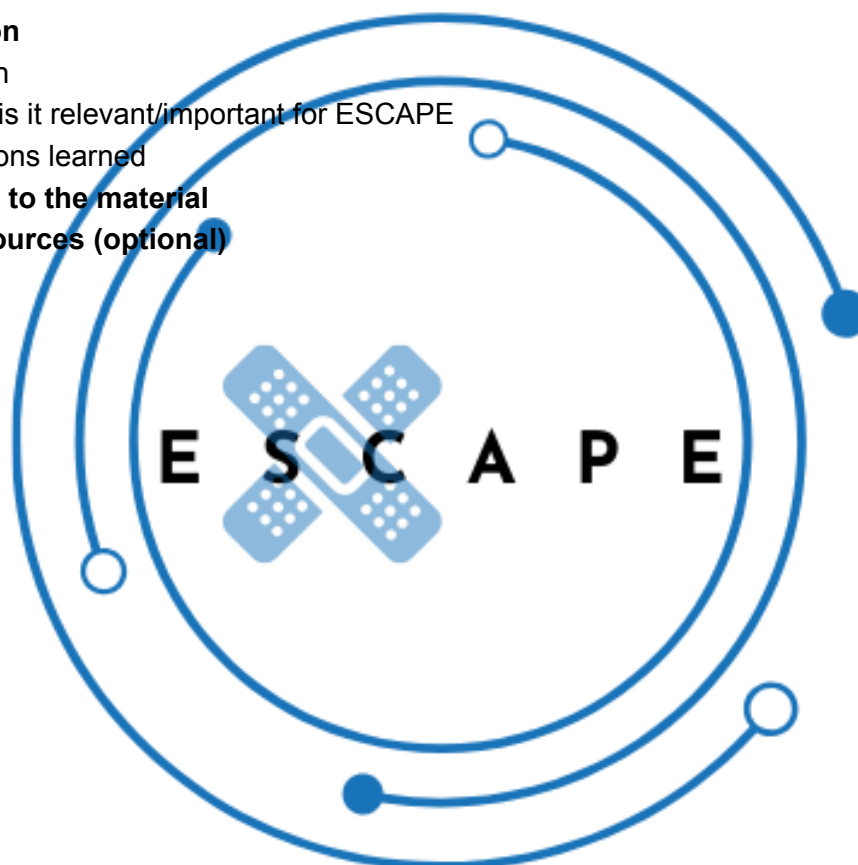
ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern	
Language	German

Table of contents

ESCAPE: Preparing healthcare professionals for cyberattacks
Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern

Language	German

1.   Name of the material and description

Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern - a European Commission action plan and communication describing the EU's strategy to strengthen the cybersecurity resilience of healthcare systems, institutions, and connected medical devices.

2.   Classification

Category	Mark if applies
Sector	☒Healthcare
	☐General public
	☐Other
Topics covered	☒Cybersecurity
	☐Data protection
	☒Prevention
Situation type	☐Impact (i.e. when it is occurring or has occurred) on patient care.
	☐Impact on all other activities not involving direct patient care.
Language of the original materials	☐Dutch
	☒English (action plan)

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern	
Language	German

	☒ German
	☐ Italian
	☐ Spanish
Type of the material	☐ Guidelines or manuals
	☐ Case or examples
	☐ Training courses
	☒ Others (policy / communication / action plan)

3. Description

It is an official communication from the European Commission presenting the European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers. The document outlines how the EU aims to strengthen resilience in the health sector through prevention, detection, and rapid response measures, supported by funding, training, and coordination across Member States.

3.1. Origin

This communication was published by the European Commission on 15 January 2025, as part of its EU action plan for healthcare cybersecurity.

3.2. Why is it relevant/important for ESCAPE

Healthcare systems are increasingly targeted by cyber threats, risking service disruption, data breaches, and patient safety. In 2023, 309 significant cyber incidents were reported in the EU health sector, with many involving ransomware.

The plan describes four strategic pillars (Prevent / Detect / Respond & Recover / Deter), along with governance mechanisms, new support centres, and funding mechanisms aimed specifically at hospitals and healthcare providers.

ESCAPE: Preparing healthcare professionals for cyberattacks
Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern

Language	German

3.3. Lessons learned

This webpage by the European Commission provides an overview of the EU's efforts to strengthen cybersecurity in hospitals and healthcare providers. It introduces the European Action Plan on Healthcare Cybersecurity and summarises its main objectives, including prevention, early detection, and coordinated response to cyber incidents. The page also links to the official communication document, funding information, and related press releases, offering readers a clear entry point to EU-level actions in this field. Overall, the webpage serves as an accessible summary and reference hub for understanding how the EU supports resilience and cybersecurity in the healthcare sector.

4. Direct link to the material

https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_de

5. Other resources (optional)

https://digital-strategy.ec.europa.eu/de/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers

https://www.enisa.europa.eu/