ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Cybersicherheit im Gesundheitswesen regulieren

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersicherheit im Gesundheitswesen regulieren	
Language	German

Table of contents

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersicherheit im Gesundheitswesen regulieren	
Language	German

1. Name of the material and description

Regulating Cybersecurity in Healthcare — a policy analysis by the Center for Security Studies (CSS) at ETH Zurich. The document examines regulatory approaches to strengthen cybersecurity in the healthcare sector, identifies key challenges, and provides recommendations for effective governance.

2. Classification

Category	Mark if applies
Sector	☒ Healthcare
	☐ General public
	☐ Other
Topics covered	☒ Cybersecurity
	☒ Data protection
Situation type	☒ Prevention
	☐ 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
	☒ German

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersicherheit im Gesundheitswesen regulieren	
Language	German

	☐ Italian
	☐ Spanish
Type of the material	☐ Guidelines or manuals
	☐ Case or examples
	☐ Training courses
	☒ Others (policy analysis)

3. Description

It is a policy paper developed by the Center for Security Studies (CSS) at ETH Zurich. It deals with how governments can regulate cybersecurity in the healthcare sector and provides recommendations to strengthen resilience, coordination, and the protection of patient data.

3.1. Origin

The material was developed by the Center for Security Studies (CSS) at ETH Zurich. It was published in December 2021 and authored by Nele Achten.

3.2. Why is it relevant/important for ESCAPE

Healthcare is highly vulnerable to cyberattacks, which can disrupt patient care, endanger safety, and expose sensitive data. Regulation plays a central role in defining responsibilities, setting standards, and ensuring security across healthcare institutions. This analysis helps ESCAPE connect cybersecurity risks in healthcare with the regulatory and policy frameworks that aim to mitigate them.

3.3. Lessons learned

Regulation alone cannot ensure cybersecurity in healthcare. It must be complemented by non-regulatory measures such as cooperation between institutions, awareness-raising, and financial or organisational incentives. Within the European Union, three main areas of regulation are particularly relevant: data protection under the GDPR, which treats health data as especially sensitive; the NIS Directive, which defines hospitals and healthcare providers

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

as essential service operators; and the Medical Device Regulation, which requires cybersecurity to be integrated throughout the entire lifecycle of medical devices.

However, several challenges remain. Definitions and implementation approaches differ across Member States, resulting in fragmentation and uncertainty. Overlapping regulatory requirements can create an additional burden for healthcare organisations, particularly smaller providers that may lack the necessary resources for compliance. Moreover, ethical and legal tensions persist between safeguarding security, protecting fundamental rights, and fostering innovation.

To address these issues, greater harmonisation of cybersecurity regulation across jurisdictions is needed. Cooperation and information-sharing between public and private actors should be strengthened, and risk-based standards should be applied in a proportionate way. Cybersecurity must become an integral part of the design, maintenance, and operation of medical devices. Finally, effective regulation should be supported by complementary measures such as funding, training, and clear governance structures to ensure that healthcare systems are both secure and resilient.

4. Direct link to the material

https://www.research-collection.ethz.ch/server/api/core/bitstreams/d2bef95e-85f9-4a1a-b985-928ef45e46c6/content

5. Other resources (optional)

https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.