ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

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	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

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	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

1. Name of the material and description

A commentary arguing that cyber-attacks—escalating in frequency and impact, especially during and after the COVID-19 pandemic—can no longer be viewed solely as IT issues. It underscores how these attacks harm **staff wellbeing** and disrupt patient care. The authors advocate for comprehensive **cybersecurity education** for all healthcare staff through **online resources, simulation, and gaming**, and emphasize the roles of national educators, policymakers, and multilateral organizations in driving these changes

2. Classification

Category	Mark if applies
Sector	☑ Healthcare (*all materials focusing specifically on the healthcare sector)*
	☐ General public *(materials targeting citizens but that are considered useful and relevant for working with the students and for the professionals, these tend to be more generic materials not targeting a specific sector)*
	☐ Other *(other materials considered relevant event though targeting a specific sector, for instance a company, but that are considered relevant for learning about cybersecurity and data protection)*
Topics covered	☑ Cybersecurity
	☐ Data protection
Situation type	☑ Prevention
	☐ Impact (i.e. when it is occurring or has occurred) on patient care. *(e.g. direct treatments, medicine distribution, etc.)*

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	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

	☐ Impact on all other activities not involving direct patient care. *(e.g. recording data, lab tests, etc.)*
Language of the original materials	☐ Dutch
	☑ English
	☐ German
	☐ Italian
	☐ Spanish
Type of the material	☐ Guidelines or manuals
	☐ Case or examples
	☐ Training courses
	☑ Others

3. Description

This is a policy-oriented commentary aimed at rethinking healthcare education to include cybersecurity as a foundational component affecting both staff and patient safety.

3.1. Origin

- ***Authors:*** *O'Brien Niki, Ghafur Saira, Sivaramakrishnan Arvind, Durkin Mike.*
- ***Submitted by:*** *Institute of Global Health Innovation, Imperial College London; Apollo Hospitals Enterprise Ltd, Chennai, India.*
- ***Published in:*** *Digital Health (2022), DOI: 10.1177/20552076221104665*

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	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

3.2. Why is it relevant/important for ESCAPE

- Highlights the evolving landscape where cybersecurity threats pose direct risks to healthcare functioning and staff welfare.
- Challenges the outdated perception that cybersecurity is solely an ICT concern—calling for **whole-system education** spanning clinical, administrative, and managerial staff.
- Promotes **innovative training methods** (online learning, simulations, serious games) for building resilience and preparedness.

3.3. Lessons learned

Commentary insights:

- ***Introduction:*** *Frames cyber-attacks as persistent, disruptive events that affect not just data but also workforce wellbeing and institutional resilience. PubMed.*
- ***Target group:*** *All healthcare professionals—from frontline clinicians to administrative staff.*
- ***Risks addressed:*** *Escalating threat landscape, normalization of ignoring cyber incidents as "IT issues only," and neglect of education and preparedness at organizational and system levels.*
- ***Solutions proposed:***
    - *Expand training via **online modules**, immersive **simulation exercises**, and engaging **gamified learning** platforms.*
    - *Mobilize support from **national educators**, **policy-makers**, and organizations like WHO to embed cybersecurity competences into wider health system education.*
- ***Tips & tricks for implementation:***

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	
Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that	
Language	*English*

- *Anchor training within **wellbeing and patient-safety frameworks** to underscore relevance to clinical outcomes.*
- *Leverage technology—**simulation scenarios, e-learning modules, serious games**—to enhance engagement and retention.*
- *Advocate for institutional and policy-level commitment to integrate cybersecurity across education curriculam.*

4. Direct link to the material

https://journals.sagepub.com/doi/10.1177/20552076221104665

5. Other resources (optional)

- ***Related commentary:** Emphasizes similar recommendations around simulation training and inclusion of cybersecurity in clinical curricula—see the Frontiers article on ransomware impact and simulation-based emergency preparation.*
- ***Further reading:** Look into evaluations of cybersecurity educational frameworks such as the ECHO framework—assessed for feasibility and usability in healthcare organizations*

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.