ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Cybersecurity in Hospitals – Legal Accountibility when Patients are harmed

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity in Hospitals – Legal Accountibility when Patients are harmed	
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	
Cybersecurity in Hospitals – Legal Accountibility when Patients are harmed	
Language	English

1. Name of the material and description

The heise online background articlue discusses who may be held criminally responsible when a cyberattack on a hospital leads to a patient harm. Using recent German and EU-developments, it explains intent vs. Negligence, management responsibilities and practical steps to reduce liability risk.

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	
Cybersecurity in Hospitals – Legal Accountibility when Patients are harmed	
Language	English

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

3. Description

The background article explores the legal and ethical implications of cyberattacks on hospitals. It provides on overview of how criminal responsibility may arise for hospital management and IT leadership when inadequate security contributes to patient harm.

3.1. Origin

The material is a background article published by heise online, the technology journalism platform of Heise Medien (independent media publisher based in Hanover, Germany). It is authored by Tilmann Dittrich and Dr. Mathias Dann, attorneys at the German law firm Wessing & Partner, specialising in medical and IT criminal law.

3.2. Why is it relevant/important for ESCAPE

Healthcare is highly exposed to cyberattacks that can disrupt care and endanger patient safety. This heise background article clarifies lega accountability for hospital leadership, linking due-care expectations to recognised standards such as B3S and the EU NIS2 framework. It helps ESCAPE translate regulatory and lega insights into practical training on documentation, oversight and staff awareness to strengthen preparedness.

3.3. Lessons learned

The article describes a heightened cyber risk for German hospitals, particularly for KRITIS facilities, illustrated by the 2019 Düsseldorf case. Although causation was not proven in that case, research indicates that care quality can worsen and mortality may rise following cyberattacks. It distinguishes crimincal intent from negligence and explains that leadership is

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.

unlikely to be found acting with intent if decisions were informed and risk adequate, whereas negligence under Sections 222 and 229 of the German Criminal Code can apply when due care is breached. Management retains ultimate and non-delegable responsibility for cybersecurity. Operational tasks may be assigned to roles such as a CISO, but oversight and accountability remain with leadership. As the benchmark for due care, the B3S standard functions as a gold standard. Implementing and documenting B3S controls strengthens a due-care defence. NIS2 is expected to extend BSIG coverage to most planned-care hospitals and to codify cybersecurity as a board-level duty, including regular training.

The practical advice in the article ist o base IT-security decisions on current and adequate information and to record the rationale and approvals. It recommends aligning policies and controls with B3S, reviewing them regularly and documenting evidence of implementation. It also calls for visible leadership oversight, preiodic training on IT risk management and clearly defined responsibilities.

4. Direct link to the material

https://www.heise.de/hintergrund/Cybersicherheit-im-Krankenhaus-Was-passiert-wenn-der-Patient-zu-Schaden-kommt-10281077.html

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.