CLOUD SECURITY

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Co-funded by the European Union

FACTSHEET – CLOUD SECURITY

1. Definition

It refers to a number of policies, controls, procedures, and technologies whose purpose is to protect cloud-based systems, data, and infrastructure1. It addresses issues such as data privacy, identity and access management, compliance, and resilience against cyberattacks from the 'cloudification' of patient data in healthcare.

2. General importance

Cloud security is a growing area of concern as healthcare increasingly adopts cloud services for data storage and processing, which require specific guidelines and security practices1. Cyber threats, breaches, or misconfigurations can expose sensitive information without strong cloud protections. Due to its shared nature, a security lapse can affect millions of users at the same time, causing not only financial and reputational damage but also compromising compliance with legal frameworks (GDPR in Europe or HIPAA in the USA).

3. Importance in health and care, and impact in quality of care

The need for technology in clinical settings has grown recently; cloud computing, telemedicine, artificial intelligence, and electronic health can often offer superior services2. Moreover, utilising cloud technology in electronic health records facilitates patients' effortless and extensive access to their health information. The use of cloud technology transforms the way physicians, nurses, clinics, and hospitals provide patients with high-quality, financially successful services3.

Cloud computing has several advantages, including easy and convenient collaboration between users, reduced costs, increased speed, scalability, and flexibility3. But, despite their numerous benefits, there are some negative aspects and challenges. Cloud computing also brings heightened risks, which can make a breach or downtime in a cloud-hosted system expose highly sensitive information, delay treatment, or even disrupt emergency services4.

4. What can I do as a healthcare professional?

- Use secure access by logging in via authorised hospital cloud platforms with strong passwords and two-factor authentication.
- Avoid sharing files with personal information outside the official cloud system.
- Be alert to cyber threats (phishing emails, suspicious links) and immediately report any irregularities
- Take part in cybersecurity training and keep up with how to respond to incidents and the impact of patient data protection.

5. More information

5.1 Learning Materials

- Cybersecurity for SMEs & self-employed (JGT-6)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-13)

5.2 Relevant Videos

This video talks about the shared responsibility model for cloud environments. It explains that businesses are responsible for keeping their applications, workloads, and data safe, while the cloud provider is responsible for keeping the security of the infrastructure that supports them.

What is Cloud Security?
https://youtu.be/jI8IKpjiCSM?si=vXJzAbIsRoj2ltDh

The next video shows how cloud computing is used in healthcare by weighing its pros, like better access and scalability, against cons, like data privacy risks and possible system dependencies.

Cloud Computing in Healthcare: The Pros and Cons
https://youtu.be/xEl_6NZuyS4?si=cFApA9QgHFCEBzPi

5. 3 Relevant Links

This article describes how a misconfiguration in the Health Service Executive's Salesforce-based vaccination portal exposed the personal and vaccination details of over one million Irish citizens, as well as internal HSE documents.

https://appomni.com/blog/saas-risks-in-healthcare-data-exposure-in-hse/

According to this article, a cloud database left publicly accessible revealed nearly 957,000 healthcare-related records, including sensitive staff and recruitment information—due to a lack of password protection.

https://www.cybersecurity-insiders.com/cloud-security-breach-leads-to-a-leak-of-957000-patient-records/

A Finnish psychotherapy company had a big data breach that made private therapy records public. The breach, which led to the clinic and its patients being extorted, cost the clinic €608,000 under GDPR for poor security and not reporting the breach in a timely manner. The fallout had a big effect on patients' trust and mental health.

https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/

6. Bibliography

Liveri, D., Athanasios, D., & Zisi, A. (2021). ENISA Cloud Security for the Healthcare Services. Enisa.
https://doi.org/10.2824/454966

Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors, 20(18), 5392.
https://doi.org/10.3390/s20185392

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal Of Medicine And Life, 14(4), 448-461.
https://doi.org/10.25122/jml-2021-0100

Guidance on HIPAA & Cloud Computing. (2022, diciembre). U.S. Department Of Health And Human Services. Recuperado 28 de agosto de 2025, de

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.