DATA BREACH

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 – DATA BREACH

1. Definition

It refers to an intentional or unintentional event that leads to the unauthorised access, disclosure, or manipulation of sensitive, confidential, or protected data, including patient data and electronic health records1. Breaches can result from hacking, phishing, misconfiguration, insider error, or physical theft.

2. General importance

In the past few years, there has been a growth in data breaches, both in frequency and severity. Approximately 46% of these incidents directly target sensitive patient information and intellectual property, often involving ransomware attacks2.

Data breaches lead to significant costs and can crush reputations because they expose personal, financial, or proprietary data. When an attack happens, businesses have to stop their systems to look into it, which causes delays, cancellations, and lost sales.

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

Cybercriminals are particularly interested in healthcare privacy breaches. This is due to the massive amount of private and financial data collected from people, which causes significant damage to both hospitals and patients. The stolen information can be helpful for identity theft and has a serious impact on patients' health and treatments3:

1. Patient safety risks arise when attackers modify patients' information, such as prescriptions and medical history, which can lead to incorrect medication administration or delays in treatment for serious illnesses.
2. According to IBM, the cost of data breaches in the healthcare sector ascends to $10.98 million. This includes expenses for medication, notifying affected patients, and forming a team to look up the data theft.
3. Legal penalties, according to HIPAA in the US and GDPR in Europe.
4. Data breaches can disrupt healthcare operations. Data breaches can take systems offline, resulting in delays, cancelled appointments, and administrative complications. Restoring the normal functioning can take weeks or months, and during this period the hospital may operate at a reduced capacity.
5. Another consequence of data breaches in healthcare is reputational damage, which may cause patients to be hesitant to share sensitive medical information. Sources estimate a 4.65% drop in patient visits post-breach4.

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.
- Encrypt sensitive data and use secure storage that adheres to regulations like HIPAA and GDPR.
- Human error is one of the most significant cybersecurity risks. Enhance employee training and keep up with how to respond to incidents and the impact of patient data protection.
- Follow a data breach response plan as soon as you detect a potential attack.

5. More information

5.1 Learning Materials

- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- Educational project on safe and responsible digital use. (IST-41)
- Regulation of cybersecurity in healthcare (BBS-23)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- 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)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)

5.2 Relevant Videos

This video explains how a data breach occurs when sensitive information is stolen and emphasises the serious risks it poses to individuals, including identity theft and financial loss.

The Dangers of a Data Breach
https://youtu.be/0kK902-ZvNM?si=88dPA3YzMOBh2Dip

This video shows that almost all healthcare organisations have experienced data breaches in the last two years, with each one costing an average of $2.4 million to resolve.

Case Studies: Healthcare Data Breach Risks
https://youtu.be/VDrWbjgM3Ik?si=ZsGCq4znqXMylOvH

In this video, the presenter discusses key cybersecurity trends for 2025 and beyond, such as emerging threats like AI-driven phishing, deepfake fraud, and shadow AI, as well as defence innovations like AI-assisted incident response and the transition to quantum-resistant cryptography.

Cybersecurity Trends for 2025 and Beyond
https://youtu.be/kqaMIFEz15s?si=vfWlFH2uQVbr4OlO

5. 3 Relevant Links

Hundreds of children's patient records were discovered in an unlocked room at Tallaght Hospital. Ireland's Data Protection Commissioner has launched an investigation into potential GDPR violations related to physical storage practices.

https://www.thesun.ie/news/15690762/children-records-data-breach-tallaght-hospital-hse/?

AMEOS, which runs more than 100 healthcare facilities in Germany, Switzerland, and Austria, had a breach in which attackers briefly gained access to patient and employee data. The organisation responded by disabling networks and engaging forensic help.

https://www.techradar.com/pro/security/european-healthcare-giant-ameos-reveals-data-breach-millions-of-users-warned-to-be-on-their-guard-heres-what-we-know?

The CNIL in France is looking into a huge breach that has affected more than 33 million people. The breach happened when third-party payment processors handled data for complementary health insurance, which exposed very private banking and personal information.

https://www.hoganlovells.com/en/publications/significant-data-breach-investigation-launched-by-cnil-affecting-over-33-million-in-france?

6. Bibliography

European action plan on the cybersecurity of hospitals and healthcare providers. (2025, 8 agosto). Public Health.

https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal.

https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Technologies, I. (2025, 7 abril). The 5 Most Alarming Healthcare Data Breaches You Need to Know. Infosprint Technologies.

https://www.infosprint.com/blogs/cybersecurity/the-5-most-alarming-healthcare-data-breaches-you-need-to-know?

Park, E., & Lim, J. H. (2025). The impact of healthcare data breaches on patient hospital visit behavior. International Journal Of Research In Marketing.

https://doi.org/10.1016/j.ijresmar.2025.01.004

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.