Interreg Danube Region

Co-funded by the European Union

DIGI4Care

Contemporary challenges in european and national health care systems

DIGI4Care

Assesing digital health and staff wellbeing

Table of Contents

Cybersecurity:
A patient-safety–centered perspective
What makes electronic medical records attractive targets for cyberattacks?
Types of cyber threats
What can be done?

Digital Wellbeing:
Definition
How can device use influence wellbeing?
Recommendations

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Learning Objectives

Understanding regulations, measures, and tools for data protection at both personal and organizational levels, as well as best practices for maintaining personal digital wellbeing.

Promoting an ethical approach to healthcare data management, increasing awareness of online threats, and supporting personal digital wellbeing.

Acquiring knowledge on protecting personal data and other sensitive information in medical environments.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Cybersecurity

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Introduction

- **"Safety" in the era of digital transformation of healthcare systems:**
  a dual concept…
- **Security of sensitive personal data / health-related data**

Preventing the compromise of data integrity, information confidentiality, and—ultimately—patient safety

- **Protection of the digital wellbeing of healthcare staff**

Reducing the negative impact of technology on mental and emotional health

- **An essential competence in contemporary professional practice:**
  the ability to navigate the digital space while ensuring safe, effective, and healthy digital practices for both healthcare professionals and patients.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Cybersecurity is not just a technical issue; it is a patient safety issue



Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Why are Electronic Medical Records (EMR/EHR) attractive targets for cyberattacks?

Demographic data, dates of birth, and unique identifiers (such as insurance numbers) can be used for identity theft, enabling criminals to obtain loans or credit cards in victims' names.

Electronic medical records may contain significant financial information.

Medical information can be used to gain access to costly healthcare services or even financial benefits (e.g., tax refunds) by impersonating patients.

A common characteristic of medical, demographic, and financial data:
the data has a very long lifespan, and monitoring its integrity is extremely difficult and complex.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Cyber Threats

Types of threats:

Ransomware
Phishing
Data breaches
Medical device hacking
DDoS (Distributed Denial of Service) attacks

Main consequences:

Operational disruptions
Risks to patient safety
Financial impact
Reputational damage

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Cybersecurity begins with individual responsibility !

Interreg Danube Region
Co-funded by the European Union
DIGI4Care



Malware

- **What should be done:**
- Do not install unverified software or applications.
- Keep operating systems up to date (enable Windows and macOS updates).
- Use antivirus software (ESET or Windows Defender).
- Do not open files from unknown USB drives.
- Do not use external hard drives that do not belong to the user or the institution.
- If a virus, slow performance, or abnormal behavior occurs, immediately inform the IT department.
- Be cautious if a paid service is offered for free.
- Use an ad blocker (including in the browser).
- Check access permissions of software and applications.

Phishing



- **What should be done:**
- Do not provide data upon request.
- Be cautious with unusual requests to change passwords.
- Verify the authenticity of email links by hovering over them with the cursor.
- Do not open unknown attachments.
- In case of a suspicious email, use the "Report spam" option to inform the IT department.
- Whenever possible, avoid accessing unknown websites.
- Check website security: https://sitecheck.sucuri.net/
- Keep the internet browser up to date.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Passwords

Common mistakes:

- Short passwords (under 8 characters)
- Use of dictionary words
- Using names, pets, or years
- Obvious links between username and password
- Replacing letters with numbers (e.g., “pa55word”)
- Using the same password everywhere

What should be done:

- Use passwords longer than 8 characters, including special characters
- Create long and complex passwords
- Use passphrases (e.g., “Is this an interesting password?”)
- Enable two-factor authentication
- Do not share passwords or explain how they were created
- Do not allow browsers to save passwords

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Passwords

- Have your data been compromised? https://haveibeenpwned.com/
- Creating a secure password: https://passwords-generator.org/
- Checking password strength: https://www.security.org/how-secure-is-my-password/
- Password management: https://keepass.info/download.html

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Open Wi-Fi Networks

What should be done:

- Use devices with properly configured firewalls.
- Use VPN connections to protect data traffic.
- Do not share files on open networks.
- Do not enter passwords, login credentials, or banking information on open networks.
- Use mobile internet whenever possible.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Device Protection

What should be done:

- Ensure proper maintenance and cleanliness of work devices.
- Protect devices from external factors (direct sunlight, dust, liquids, strong magnetic fields, etc.).
- Lock the screen when the device is unattended (WIN + L / Lock Screen / Touch ID on Mac).
- Do not leave devices unattended while charging.
- Use strong passwords or biometric authentication.
- Prevent unauthorized access to devices.
- Be cautious with unknown storage media.
- Dispose of external hard drives securely.
- Store data in multiple locations.
- Do not use work devices for sensitive private content

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

1. What is the main reason healthcare data is a high-value target for cybercriminals?

A) It is easy to access
B) It contains personal and financial information
C) Healthcare organizations do not invest in security
D) Cybercriminals prefer healthcare over other industries

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

2. Which action should be taken to secure a healthcare system against cyber threats?

A) Using weak passwords to simplify access
B) Sending patient information via unencrypted email
C) Regularly updating software and systems
D) Storing all passwords in an unprotected document

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

3. What are the potential consequences of a cyberattack on healthcare institutions?

A) Minor inconveniences
B) Operational disruptions, patient safety risks, and financial losses
C) No significant impact
D) Increased productivity

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

- **4.** Which of the following is an example of good cybersecurity practice for healthcare professionals?
  A) Reusing the same password across multiple systems
  B) Verifying recipients before transmitting sensitive data
  C) Disabling security software to increase speed
  D) Ignoring suspicious emails or links

Exercise: Practical Data Protection Quiz

5. How can digital technology negatively affect personal wellbeing?
A) It always improves work–life balance
B) Compulsive checking and media multitasking can increase anxiety
C) Notifications improve focus and attention
D) It ensures better sleep quality

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

6. What is end-to-end encryption and why is it important in healthcare data sharing?
A) A method of storing data without encryption
B) Encrypting data during transmission, ensuring access only for authorized users
C) Allowing anyone on the network to access patient data
D) Preventing data sharing between systems

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Exercise: Practical Data Protection Quiz

- **7.** Which measure should be adopted to improve digital wellbeing?
  A) Keeping all notifications enabled for immediate responses
  B) Intentionally managing technology use to reduce distractions
  C) Avoiding breaks from technology use
  D) Ignoring work–life balance and focusing solely on productivity

Exercise: Practical Data Protection Quiz

- **8.** What should be avoided when sharing sensitive healthcare information?
  A) Using two-factor authentication
  B) Sending unencrypted files via email
  C) Regularly updating passwords
  D) Confirming the recipient's identity before sending

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

DIGI4Care

Digital Wellbeing

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

Digital Wellbeing

- A good or satisfactory state of existence, characterized by health, happiness, and prosperity.
  Digital technology can either support or disrupt this balance
- Source: Google – Digital Wellbeing Product Experience Toolkit

How does device use influence our wellbeing?

DISADVANTAGES:

- Increased stress
- Increased anxiety
- Negative impact on memory
- Difficulty maintaining intentions
- Disruption of personal interactions
- Work–life imbalance

ADVANTAGES:

- Staying connected with others
- A tool for learning and continuous updating
- Support for wellbeing

Interreg Danube Region
Co-funded by the European Union
DIGI4Care

In Focus: INTENTIONAL USE

Assessing and monitoring usage habits → Setting clear limits → Reducing distractions → Using self-control tools

Improving digital wellbeing at work → Strengthening privacy and data security → Mindful use of social media → Improving body posture

Protecting visual health → Considering overall health status → Consulting the digital wellbeing checklist

Source: Visitor Analytics – *Checklist Your Digital Wellbeing*

- Do digital wellbeing settings (notifications, work/personal accounts, social media, screen settings, etc.) support intentional use?
  → Adjust settings.
- Is there a desire to support physical or mental wellbeing through planning or monitoring apps?
  → Explore options and test them (while checking app credibility).
- Is there a need to improve privacy and data protection (password managers, privacy settings, VPN, DNS encryption, etc.)?
  → Strengthen device security.

Conclusion

- Safety begins with recognizing threats, and cyberspace is no exception. Understanding attackers' motivations and tools is essential for protecting patient data—and ultimately, patients themselves.
- Digitalization is not a future scenario; it is our current living environment.
- Cybersecurity is not solely the responsibility of IT specialists.
- Applying appropriate measures in daily practice may seem time-consuming, but it is essential for the safety of patients and healthcare staff and can, in reality, become a time-saving factor.

Interreg Danube Region
Co-funded by the European Union
DIGI4Care