

Co-funded by the Erasmus+ Programme of the European Union 	BeWell – Cybersecurity for Healthcare Staff competence matrix	
EQF Level	3-5	ESCO: Cyber security (Knowledge)
Aggregated Units of Learning Outcomes	BeWell – U1.4	Cybersecurity for Healthcare Staff

		BeWell		
Generic Title of the Unit:		U1.4 – Cybersecurity for Healthcare Staff		
Description:		The healthcare industry faces many cyber threats, potentially jeopardising patient confidentiality, data integrity and availability. These concepts form the backbone of cybersecurity in healthcare. Breaches not only disrupt services but can lead to severe consequences for both patients and healthcare facilities, from identity theft to significant financial and reputational damages. By understanding and rigorously implementing cybersecurity measures, healthcare professionals uphold their ethical duty to safeguard patient data, fostering trust and ensuring quality care.		
EQF Level:		3-5		
Learning Outcomes				
BeWell U-1.4	Training Module Code	Competence (Autonomy and responsibility)		
		Knowledge		Skills
1.1 General concept of cybersecurity	TD04-M1	Is able to use the general concept of cybersecurity to protect patient data in their daily work		
		Understands the general concept of cyber security and its importance in the healthcare industry		Identifies the most common forms of cyber threats such as malware (viruses, worms, and Trojans), social engineering (phishing, pretexting), ransomware Acts to present the most common forms of cyber threats when working with patient data and other types of sensitive information
1.2 General Data Protection Regulation (GDPR) and cybersecurity	TD04-M2	Is able to understand, explain and use the purpose and key principles of the GDPR and how it relates to their work with sensitive data		
		Has a general understanding of the purpose and key principles of the GDPR, its connection to cybersecurity and its implication for their work		Follows the requirements for healthcare organisations when collecting, storing and sharing patient data
		Understands the rights and responsibilities related to their handling and protecting of patient data under the GDPR		

		Knows the content of the requirements for healthcare organisations when handling and protecting patient data (informed consent, right to access, rectify and erase data)	
1.3 Safe password management and email use	TD04-M3	Is able to practice safe password management and safe use of emails to protect themselves against cyber threats.	
		Understands the importance of strong passwords and its role in securing sensitive information	Practices safe password management at work by creating strong and unique passwords and avoids common password pitfalls
		Knows the most central best practices for creating strong passwords, the importance of two-factor authentication and the most common authentication pitfalls	Verifies sender email addresses when receiving emails and identifies phishing attacks
		Has a general and superficial understanding of additional security measures such as multi-factor authentication and password managers	Follows safe browsing practices such as using secure websites when at work and when using equipment from work
1.4 Secure use of mobile devices	TD04-M4	Is able to use mobile devices in a work setting while minimising the most common cybersecurity threats	
		Understands the importance of implementing security measures for mobile devices, including encryption and device passcodes	Avoids using public Wi-Fi networks when using work-related devices and working on work-related tasks and uses reliable VPNs (Virtual private network) instead
			Does not share personal information related to their digital identity to anyone
			Uses data encryption software

			Avoids potential vulnerabilities when using mobile devices for work-related tasks
1.5 Reporting security incidents	TD04-M5	Is able to recognise and explain to others the most common signs of cyber-attacks (slow internet, unexpected error messages)	
		Understands the importance of reporting security incidents and knows how to do so	Follows the correct procedures when responding and reporting a cyber-attack
			Isolates infected devices
		Knows the most important consequences of failing to report security incidents	Acts responsibly when preserving data by doing data backups and cooperating with IT professionals