



Cybersecurity for professionals. Bezpieczeństwo w cyberprzestrzeni dla profesjonalistów.

1. IMPRINT

Academic Year	2026/2027
Department	Faculty of Medicine
Field of study	Medicine
Main scientific discipline	Medical science
Study Profile	General academic
Level of studies	Uniform MSc
Form of studies	Full time studies
Type of module / course	Non compulsory
Form of verification of learning outcomes	Completion
Educational Unit / Educational Units	Department of Medical Informatics and Telemedicine 00-581 Warszawa, Litewska 14/16 phone (+48) 22 116 92 44 e-mail: zimt@wum.edu.pl
Head of Educational Unit / Heads of Educational Units	Andrzej Cacko, MD, PhD
Course coordinator	Joanna Michalik, MD, e-mail: joanna.michalik@wum.edu.pl
Person responsible for syllabus	Joanna Michalik, MD, e-mail: joanna.michalik@wum.edu.pl
Teachers	Dr hab. n. med. Andrzej Cacko; andrzej.cacko@wum.edu.pl Lek. Joanna Michalik; joanna.michalik@wum.edu.pl Marta Nowak; zimt@wum.edu.pl

2. BASIC INFORMATION

Year and semester of studies	IV-V year, winter and summer semester	Number of ECTS credits	2.00
------------------------------	---------------------------------------	------------------------	------

FORMS OF CLASSES	Number of hours	ECTS credits calculation
Contacting hours with academic teacher		
Lecture (L)		
Seminar (S)	30 (e-learning)	1.2
Classes (C)		
e-learning (e-L)		
Practical classes (PC)		
Work placement (WP)		
Unassisted student's work		
Preparation for classes and completions	20	0.8

3. COURSE OBJECTIVES

	In the era of digitalised healthcare, the ability to use technology safely has become a competence as important as medical knowledge. This optional course will prepare you to work in an environment where electronic documentation, telemedicine, and networked devices are part of everyday practice. A physician aware of cyber threats is a professional whom patients can trust.
O1	This optional course teaches students how to recognise common cyber threats in medical facilities so they can protect themselves and their patients from cyberattacks. You'll learn about the latest cybersecurity solutions and how to assess which ones are worth implementing in your future practice.
O2	We will examine how new technologies, namely medical apps, wearable devices, and IoMT systems, can support diagnosis and treatment, but also pose risks to patient privacy and the security of medical systems. We will discuss principles for the safe use of smartphones, tablets, and computers, as well as applications and IT systems in everyday medical practice.
O3	The goal of the elective is to raise students' awareness that personal data protection is not only a legal requirement but an element of patient safety and medical professional ethics. We will discuss how patient data can be compromised in everyday practice and what procedures should be implemented to report a personal data breach.

4. STANDARDS OF LEARNING – DETAILED DESCRIPTION OF EFFECTS OF LEARNING

Code and number of the effect of learning in accordance with standards of learning	Effects in the field of:
Knowledge – Graduate* knows and understands:	
B.W26.	basic information about technology and biostatistical methods used in medicine, including medical databases, spreadsheets and basics of computer graphics
B.W28.	applications of the contemporary telemedicine as a tool supporting a medical doctor's work

Skills– Graduate* is able to:

B.U10.	use databases, including online databases, and search for the required information using provided tools
--------	---

* In appendix to the Regulation of Minister of Science and Higher education from 26th of July 2019 „graduate”, not student is mentioned.

5. ADDITIONAL EFFECTS OF LEARNING *(non-compulsory)*

Number of effect of learning	Effects in the fields of:
------------------------------	---------------------------

Knowledge – Graduate knows and understands:

K1	the process of the development of new specialities in the medical sciences and the achievements of leading representatives of Polish and global medicine
K2	legal regulations concerning the management of medical records, as well as the criminal, civil, and professional liability of physicians

Skills– Graduate is able to:

S1	draw conclusions based on a critical analysis of medical and cybersecurity literature, including in English
----	---

Social Competencies – Graduate is ready for:

SC1	using reliable sources of information
SC2	respecting medical confidentiality and patients' rights

6. CLASSES

Form of class	Class contents	Effects of Learning
(e-L) seminars	S1. – Seminar 1 – The concepts of cybersecurity, cyberspace, and cybercrime. The most significant types of threats encountered on the Internet and examples of cyberattacks targeting individuals, businesses, and public institutions. The specific nature of threats in the healthcare sector. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S2. – Seminar 2 – The Polish national cybersecurity system. The cybersecurity strategies of the EU and Poland. Criminal liability for crimes committed in cyberspace. Legal obligations regarding cybersecurity in the operations of healthcare institutions. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S3. – Seminar 3 – Criminal and investigative issues. Digital evidence. Discussion of the types of information that may constitute evidence, the principles of data preservation, and the necessity of maintaining data integrity. Examples of digital traces left in healthcare institutions' IT systems. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S4. – Seminar 4 – Cybersecurity incidents and their management. Stages of incident management. Restoring proper system operation. The importance of documentation and concluding the future. Case studies. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.

	S5. – Seminar 5 – Phishing and social engineering as cybersecurity threats. The impact of phishing on patients, employees, and healthcare institutions. Guidelines for safe practices and phishing prevention. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S6. – Seminar 6 – GDPR and personal data protection. Responsibilities of healthcare personnel and healthcare institutions. Zero trust in healthcare: application of the zero-trust model to electronic health records and medical devices. Credit from seminars 1–6: summary test (online) Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S7. – Seminar 7 – Workshop (1): Strategies of attacks on hospital or other medical systems. Analysis of selected cases. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S8. – Seminar 8 – Workshop (2): Preventing and responding to digital attacks. Analysis of selected cases. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S9. – Seminar 9 – Workshop (3): Personal data breaches. Analysis of selected cases. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.
	S10 – Seminar 10 – Workshop (4): Personal data breaches – prevention and response. Scenario analysis. Asynchronous e-learning, eWUM platform, specified weeks	B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.

7. LITERATURE
Obligatory
1. Lectures and educational materials prepared on WUM e-learning Platform.
Supplementary
1. Selected materials published on the websites of NASK, the e-Health Centre, the Polish Personal Data Protection Office, and the Ministry of Digital Affairs
2. Selected materials published on the websites of the WHO and the European Union Agency for Cybersecurity (ENISA)

8. VERIFYING THE EFFECT OF LEARNING		
Code of the course effect of learning	Ways of verifying the effect of learning	Completion criterion
B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.	Completion of e-learning assignments and activities, including two optional workshops	Completion of e-learning modules - obtaining at least 51% of the points in the indicated assignments and activities.
B.W26., B.W28., B.U10., K1, K2, S1, SC1, SC2.	Credit (Passing the theoretical part, seminars 1-6): e-test	Obtain at least 51% of the points. The final grade is a mark of the e-test and seminars. Grade range: 2.0 (ndst) - up to 51% of points, 3.0 (dst) - 51.1%-60% of points, 3.5 (ddb) - 60.1%-70% of points, 4.0 (db) - 70.1%-80% of points.

9. ADDITIONAL INFORMATION

The full optional course lasts one semester and is conducted in the winter or summer semester. Students may sign up for only one optional course edition.

The minimum number of students required to start the optional course in a given semester is 20.

An unlimited number of students can participate in the optional course.

Seminars schedule:

Materials will be provided sequentially.

In the winter semester (Edition 1), starting on 19 October, 2026. The course will end on 24 January, 2027.

In the summer semester (Edition 2), starting on 29 February, 2027. The course will end on 6 June, 2027.

All course topics and credits are completed via eWUM (e-learning.wum.edu.pl), the university's e-learning platform.

Before the course begins, each student must verify that they can log in to the WUM Platform. If you encounter any login problems, please get in touch with the person responsible for the platform's operation (e-learning@wum.edu.pl).

Please direct technical issues related to the course, as well as any questions or requests, to the course instructor: Joanna Michalik; joanna.michalik@wum.edu.pl.

The course consists of six online seminars, a final test covering seminars 1–6, and four elective workshops, of which the student must complete at least two.

Each participant has three attempts at the final test. The higher score counts toward the grade.

The course grade is determined by the final test score and the grade for the assignment completed in the workshop the student chooses. The final grade is the average of both scores, provided that neither score is a failing grade.

If a student cannot take the final exam by the designated deadline, they must email the course instructor to request an excused absence. The student must submit the request no later than three [3] days after the circumstances that prevented them from taking the final test occurred. Failure to submit the request by the specified deadline will result in the absence being considered unexcused. You may submit an excuse after the deadline if you were unable to submit it for valid reasons; in such cases, submit the document as soon as the reason for the absence ceases to exist.

An unexcused absence from the final exam constitutes grounds for recording a failure for the course in the given term.

If a student has an excused absence from the final exam, they may take the exam on the next date scheduled by the department.

If a student receives a failing grade, they are entitled to two make-up exam dates. If a student fails to pass the course by the final date set by the department in a given academic year, they will not receive credit for the course.

The department also has a Students' Club MedIT, which brings together students who want to improve their knowledge of medical informatics, artificial intelligence, and advanced computer methods in medicine.

If you are interested, please get in touch with the tutor: Jakub Rokicki (jakub.rokicki@wum.edu.pl).

Medical University of Warsaw has property rights, including copyright, to the syllabus. The syllabus may be used for educational purposes at the MUW only. Using of the syllabus for other purposes requires consent of the MUW.

ATTENTION

The final 10 minutes of the last class of the block/semester/year should be allotted for students to fill out the Survey of Evaluation of Classes and Academic Teachers