



Studies module

Health Information Systems training and certification implementation for higher education

CC BY-NC



KAUNAS UNIVERSITY OF TECHNOLOGY

STUDY MODULE PROGRAMME (SMP)

Module Code	Branch of Science	Progr.	Registr. №.	Accredited until	Renewal date		

Entitlement

Health information systems and workplace IT security

Prerequisites

It is required that course participants have basic digital literacy competences, like computer essentials and online essentials skills.
Participants could be health education students and health sector staff like doctors, nurses and healthcare support staff, etc.

Main aim

By taking this bended training course participants will acquire knowledge about heath information systems (HIS) and about workplace IT security. After training participants will be prepared for ECDL (European Computer Digital Literacy) certification. After this course participant will:

- Understand the key features of a Health Information System (HIS).
- Use a HIS safely and efficiently.
- Understand the ethics, rules and regulations relating to HIS.
- Understand confidentiality, security and access control when using a HIS.
- Understand and interpret electronically recorded data.
- Gain common IT security knowledge.
- Understand workplace security.
- Understand about computer' safe usage and browse the Internet safely.

Learning outcomes

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
1.	Concepts	Lecture, examples, practical exercises (tasks), recommended literature for reading and links to videos	Self evaluation questions, knowledge evaluation test, exam, laboratory notes and report
1.1.	Understand what is e-services, how they work, connection to the systems ways, understand that logs of users of can be identified, understand that statistic information could be reviewed	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.2.	Understand that information systems can be installed to the computer or server (could be used by connecting via browser). Understand scalability of HIS, such as office /department based, local facility based, regionally based, nationally, or internationally based.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.3.	Understand the meaning of reliability, security, authorization to view data from your own authorized source rather than an external source	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.4.	Understand what is information systems and role of information system. Know some examples of information systems, like search engines, enterprise resource planning, Healthcare Information System (HIS), health management information system.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.5.	Understand that HIS are used for holding and updating patient-related information and records, clinically as well as administratively oriented. Understand that a HIS may be made up of patient, personal or population records.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.6.	Understand that Information systems data could be used for systems' automated tasks, like	Lecture examples,	Self-evaluation questions

This project has been 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.



Erasmus+

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
	automatic diagnosis determination, management plans, statistic information generation with respect to individual patients, and testing and procedures that result from these plans. Nevertheless HIS only supports but does not replace clinical judgment.	recommended literature for reading and links to videos	
1.7.	Understand different data sources in the HIS: Civil registration, Population surveys, Individual records, Service records, Resource records. Understand the relationship between population records and personal health records.	Lecture examples, recommended literature for reading and links to videos	Self-evaluation questions
1.8.	Understand benefits of Healthcare delivery through a HIS such as more reliable, timely information leading to better patient care.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.9.	Understand that HIS are made up of different parts such as: Electronic Health Record, ordering, imaging, prescribing and laboratory systems, PACS, Ultrasound, results-based, decision-support, multimedia and billing where appropriate. Understand that these systems have link with each other and can share parts of the data with each other.	Lecture, practical tasks if there is possible, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.10.	Know some of the key qualities of a HIS such as: accessible, reliable, rapid access, shared view, up-to-date, accurate, provides for a continuum of care, efficient, and incorporates some important safety features.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
1.11.	Identify or know about key functions or tools of HIS such as: scheduling, updating patient data, giving prescriptions for medicine and procedures. Limitations of HIS systems, like lost of direct patient – doctor contact, lack of suability in results, less human, more machine oriented descriptions using standard expressions to facilitate easy search.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
	Summary: finished this part students have to understand basic principles about e-services, HIS, how data are stored and how IS works,	Basically there should be used presentations on	Knowledge assessment should

This project has been 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.



Erasmus+

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
	<i>secure connection to the IS ways, understand automated tasks performed by IS, know that there are different IS connected with each other, understand advantages and limitations of information systems.</i>	theoretical lectures by demonstrating some examples of real systems, show videos from Youtube about IS if there is a possibility. Discussions also could be used as a teaching method.	be used by finishing confidentiality part.
2.	Confidentiality		
2.1.	Understand that patient data could be accessible by multiple entities: insurance companies, patients providers, drugstores in appropriate amount of data and appropriate Access rights. Understand that patient data must be processed on need-to-know basis: access only to patient information when necessary; access only to items that are need-to-know; access only to information that is right-to-know, awareness of concept of personal accountability. Recognise the distinction that system access does not imply authorization to view or use.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
2.2.	Understand the patient's right of (implied or explicit), issues such as sensitivity in dealing with patient data in relation to family members and others. Appreciate patient right not-to-know issues.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
2.3.	Understand that local legislation gives patients or to legal representatives the right to review and amend their own records.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
2.4.	Understand national requirements when to report and inform appropriate authorities of patient specific data / rules and constraints, public health, notifiable diseases.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

This project has been 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.

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
2.5.	Understand that medical staff have to adhere to the key principles of security within HIS such as awareness of systems vulnerability, requirement for formal agreement to organisational security policy.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
2.6.	Understand that medical staff has to adhere an organisational security policy: it can have personal, professional and organisational outcomes.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
2.7.	Understand that medical staff has to adhere an organisational rules to inform appropriate staff about security breaches and threats.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
	<p><i>Summary: finished this part students have to understand about confidentiality, access rights, know about internal organisational rules regarding confidentiality, understand that patient data must be processed on need-to-know basis, understand when and to whom patient data could be discovered, when and who must be informed in particular ways.</i></p>	<p>Basically there should be used presentations on theoretical lectures by demonstrating some examples of real systems, show videos from Youtube about IS if there is a possibility. Discussions also could be used as a teaching method. During discussions scenarios method could be used.</p>	<p>HIS concepts and confidentiality are theoretical parts, acquired knowledge could be evaluated by performing exam or by using online knowledge evaluation test. In order to understand material, one or two workshops could be organised, where students could give presentations about IS, HIS and confidentiality. Students could work in small groups. Recommendations about theoretical questions are described in the annex.</p>
3.	HIS usage	Lecture, practical tasks,	Self evaluation questions,

This project has been 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.



Erasmus+

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
		examples, practical exercises (tasks), recommended literature for reading and links to videos	knowledge evaluation test, exam, laboratory notes and report
3.1.	Know how information systems could be used for performing everyday tasks, like connection to the system, navigation, looking for appropriate records, verifying and locating them. Know how to select, review and edit patient records based on particular criteria about the patient or his treatment history. Identify the authorship and hospital of an entry in a record. Identify different modes (automated) of data entry.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.2.	Know how to enter new records, fill with data. Understand when two records are created and know how to merge them.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.3.	Know how to register patient for the next visits and cancel the visit if the need arises.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.4.	Know how manage automatic system alerts, reminders, validation checks etc. Understand who, when and how deals with them. Understand when the appropriate decision is needed.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.5.	Know how to perform filtering, creation and query of clinical reports and reservation of hospital resources. Review specific reports, like x-ray, ECG, CT-Scan, blood result etc.	Lecture, practical tasks, examples, recommended	Self-evaluation questions

This project has been 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.

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
		literature for reading and links to videos	
3.6.	Know how to prepare records for printing and know how to securely print (secure print option on the shared department printers, i.e. PIN code in the printer).	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.7.	Understand that medical staff have to adhere to the organisational rules by transmitting patient data to other departments, medical institution, to patients and their relatives in any format (printed materials, e-mails, etc.). They have to understand that there must be consent of patient for transmitting medical data for third parties.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.8.	Understand that the patient record is a legal document and no information can be erased it can amended but not changed.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
3.9.	Understand who has the authority to create new records. Understand the importance of HIS system audit trail.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
	<i>Summary: finished this part students have to understand how to work with information systems. It is recommended to use real health information system in order perform practical tasks.</i>	It is recommended to invite external lecturer, who works with real health information system and practically show how their information system works.	Online test could be used for knowledge assessment. Hotspot questions have to be used in order to understand how HIS works, theoretical questions should be used as well. Recommendations about hotspot and theoretical questions are described in the annex.

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
4.	Common IT Security Knowledge	Lecture, examples, practical exercises (tasks), recommended literature for reading and links to videos	Self evaluation questions, knowledge evaluation test, exam, laboratory notes and report
4.1.	Know about advantages and disadvantages (risks) of information technologies and the internet. Understand why information systems users and administration staff have to know about possible risks.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.2.	Know about cybercrimes, understand that is financial frauds, how illegal activity could be performed on the workplace, know about viruses, malware, types, how viruses could get into device. Know about hackers, understand hacking risks (possibility to hack user computer, system, network) and reasons. Know about avatars and possible risks.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.3.	Be aware about social engineering and its methods for discovering information. Know about discovering information in unauthorised ways (phone calls, pretenders, phishing, spyware). Understand that social engineering could be used in the company, hospital. Know about unauthorised access to the computers and other devices without user's approval; know about lottery scams. Understand about remote access to the systems, and who is allowed to use them. Do not discover this information to third parties without official permission.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
4.4.	<p>Know the term Identity; be aware about identity theft and theft methods. Understand what is personal data, what data could be published. Understand that systems on the internet could track and assemble information about users devices, activities, location (location history), could record searching history (record voices and videos), provide adds according user' behaviour preferences.</p> <p>Be aware about spyware, fraud advertisement, Trojans. Know various ways how malicious software, trojans and fraud advertisement could get into device. Know about keyboard spy, know types of keyboard keys (software and hardware tools).</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
4.5.	<p>Know about reasons and consequences of identity and personal data thefts in the workplace and on the internet (fraudulent information usage, threat of information loss, sabotage). Know about threats associated with personal data disclosure. Understand that it is not allowed to share sensitive information about company or clients to third parties (relatives, friends, colleagues, representatives of competing companies etc).</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
4.6.	<p>Know various ways how personal identity could be stolen, like phone calls, online methods (emails with fake links, emails from fake personal accounts with real name and surname of employee (company have to use only companies emails), understand about social network using for companies purposes, instant messaging usage in the workplace). Options and parameters for information disclosure. Understand what is the fascination to disclose private information on the internet. Understand that login data to company systems, like emails, social network, instant messaging programmes could not discovered to other people. Know about skimming, shoulder surfing, information diving, deleted information recovering methods.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
4.7.	Be aware of privacy protection legal acts. Know basic legal acts related with data protection.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.8.	Know about organisational data management rules, data privacy principles, confidentiality. Know what is staff confidentiality agreement, when else is a confidentiality agreement used.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.9.	Understand that it is necessary to exercise critical thinking about content and identities on the internet. (i.e. blogs, Wikipedia, social networks, forums, etc.). Know who you should contact if you discovered inappropriate information about you or your organisation on webpages or social network. Know who to contact if you get phishing emails.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.10.	Be aware of the responsibility for own actions on the Internet: do not publish the information without permission, be responsible by writing comments, do not download illegally music, movies, etc.). Know about possible consequences and personal responsibility.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
4.11.	Know about netiquette and other basic codes of conduct in the cyberspace. Know emails writing recommendations, writing comments etiquette, understand that device information (like computer IP address) could saved on the server or/ and published with comment. Understand when emails could become as a spam.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
	<p><i>Summary: finished this part students have to acquire basic IT security knowledge, possible threats using computer and internet, how about social engineering and used methods, know various ways how personal identity could be stolen, be aware of privacy protection legal acts. Know about staff confidentiality agreements, understand about responsibility related with data disclosure to third parties.</i></p>	<p>Basically there should be used presentations on theoretical lectures, show videos from Youtube if there is a possibility. Discussions also could be used as a teaching method. During discussions scenarios method could be used.</p>	<p>Knowledge assessment should be used by finishing confidentiality part.</p>
5.	Computer and Internet security	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self evaluation questions, knowledge evaluation test, exam.
	Computer security		
5.1.	<p>Know about importance of updates for operating system, programs, browsers and antivirus software. Understand that ignoring of programs' updates could have security consequences.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
5.2.	<p>Know purpose of antivirus program usage on the devices. Know that it is not allowed to disable antivirus in any case even user wants to open important document or website. In such ways he should know to contact IT administrator or other responsible person, who can help to open such documents.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
5.3.	<p>Know about possibility to lock or limit documents from editing, like in word or excel documents, know how to enable and disable document proofing. Know how to set password for compressed files, documents opening and editing.</p>	<p>Lecture, practical tasks, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>

This project has been 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.



Erasmus+

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
5.4.	Identify main symptoms of virus infection: unusual slow start-up operating system, performance operating system, disturbing advertising warnings, self-opening windows that were not requested, application won't start or do not response, cannot connect to the Internet or it runs very slowly, disks are not accessible an etc. Know what has to be done and in what order, if you suspect that computer system is infected (like first of all to contact IT administrator).	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
5.5.	Understand the benefits and purpose of data backups.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
	<i>Summary: finished this part students have to acquire basic knowledge about how to use computer securely, understand why operating system and programs have to be updated, understand why antivirus have to be used in the computers and smart devices. Students should know main symptoms of virus infections, know what has to be done if device is infected. Know about documents editing and opening limitations, understand the benefits and purpose of data backups.</i>	Basically there should be used presentations on theoretical lectures, show videos from Youtube if there is a possibility. Discussions also could be used as a teaching method. During discussions scenarios method could be used.	Knowledge assessment should be used by finishing confidentiality part.

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
	Internet security		
5.6.	Know how to safely browse the Internet. Know differences between http and https, know meaning of websites certificates, know types of certificates. Be able to safely connect to e-services and secure environments. Know how to recover lost passwords. Know that it is required to disconnect when user leaves IT system. Know about option to browse in the private window.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
5.7.	Know about cookies, password storage on the computer or in the browser, know that other persons can review stored passwords.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
5.8.	Identify possible fraudulent e-mail, unsolicited email. Know about dangers when opening attachments that may contain a macro or an executable file. Know that emails with sensitive information could not be forwarded to other people. Know about scam, hoax, chain letters.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
5.9.	Be able to identify fake websites that could be opened by clicking a link from emails, on social media and etc. Understand that it is not allowed to open such links, know about possible consequences. Know about consequences if you discover personal or companies' sensitive data on such website. Know who to contact if you discovered fake website.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
	<p><i>Summary: finished this part students have to acquire basic knowledge about how to use internet securely, understand why access to systems data couldn't be saved on the browser and documents. Know about safe communication via emails. Know and identify fake websites and reasons why they are used by cybercrimes.</i></p>	<p>Basically there should be used presentations on theoretical lectures, show videos from Youtube if there is a possibility. Discussions also could be used as a teaching method. During discussions scenarios method could be used. These should be used at least one practical lecture about computer and internet security.</p>	<p>Online test with hotspot and theoretical questions could be used for knowledge assessment. Recommendations about hotspot and theoretical questions are described in the annex.</p>
6.	<p>Organisational Workplace Security</p>	<p>Lecture, practical tasks, examples, recommended literature for reading and links to videos</p>	<p>Self evaluation questions, knowledge evaluation test, exam.</p>
6.1.	<p>Be familiar with the organisational security policy in the institution: guidelines of device usage in the workplace (know about possibility to use workplace devices for personal purposes). Understand that employer could record and track employees devices activities. Know about company policy for bringing devices home. Know about mobile devices (like, smartphones, tablets) usage policy.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
6.2.	Know about safeguarding printed documents, keeping and managing documents. Know that printed important and confidential documents with sensitive data cannot be left on the printer or left without supervision. Know about consequences if these documents would be read or stolen by unauthorised persons. Understand that printed confidential or other paper documents, like patients records, have to be kept safely according to the organisational rules of the company.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.3.	Know about company policy to bring and use own personal devices (like smartphones, tablets, USB flash drives) on the workplace. Know about company' organisation rules to use external drive devices (be careful or do not use clients or other people USB flash drives). Understand that malware or spyware could be recorded to the external drive device. Know about company policy for connecting own personal devices to the Internet and about consequences.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.4.	Know about company policy for installing apps to the company computers, smartphones and tablets (understand term application permission; know about consequences if employee installs apps from unknown sources). Understand risks connecting these devices to the public access points via Wi-Fi. Know about possible threats and consequences if someone hacks company device or if device will be infected by virus (personal data theft, unauthorised information storage without permission, hidden fees or location tracking).	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.5.	Understand the purpose and meaning of user authorisation when he connects to the device or information system. Understand that users has could have different roles and different access to the same system. Know methods how to connect to the devices or information systems safely, like username and password, PIN, chipcard, login using biometrical data, multi-factor authentication, one-time password.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

This project has been 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.

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
6.6.	Know that it is not allowed to leave logged in devices and information systems unattended even for the short period (when leaving the workplace the computer have to be locked, chipcard have to be removed from the device).	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.7.	Understand and ensure that unauthorised persons have no possibility to track employees' screens (each user should protect his screen from shoulder surfing). Understand that monitors have to stand in such way that clients or patients have no possibility to track employees' activities. Know about safe mobile devices usage: do not enter passwords or other sensitive information if there are cameras behind users' back or other persons could track screen.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.8.	Know about guidelines for creating and managing strong passwords. Be able to create complex passwords, know how many symbols have to be in the password, what symbols used in the password could make password stronger. Know how to create strong but easy remembering passwords, understand logins and passwords storage. Understand that passwords have to be changed regularly. Know how to identify if password is strong.	Lecture, practical tasks, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.9.	Understand that user authorisation to devices, programs and information systems is used for identification of particular user, and authorisation data or chipcard cannot be revealed to colleagues or to other persons. Know about consequences if unauthorised person connects with login data of particular employee.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions
6.10.	Understand that installing any software on the companies' device is allowed only for companies' responsible person (like IT administrator) or third part company, which has agreement to supervise IT. Understand about illegal software installation and risks to lose information, risks to hack device or system, risks to spy computer and etc.	Lecture, examples, recommended literature for reading and links to videos	Self-evaluation questions

This project has been 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.



Erasmus+

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
6.11.	<p>Know about periodical companies' devices revision and who performs this revision. Understand consequences if unauthorised person connects to companies' devices.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
6.12.	<p>Know about workplace ethics: distinguish personal data from business or company data; know what data can be stored on the companies' device and know about consequences of storing inappropriate data. Understand that companies' and clients' data cannot not be disclosed to the third parties.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
6.13.	<p>Know about collaboration tools. Know how to share documents on the internet to authorised persons, how that several users can work with the same document at the same time when the document is published on the clouds. Know about risks to loose sensitive information by sharing documents (sharing settings, sharing to whole people, sharing to particular people). Know that documents should to be deleted from the clouds drive when the document is finally prepared and do not used any more (it should be identified in the organisational rules). Know about possibility to share printers and desktop to colleagues. Knows risks of the device sharing. Know about data control, potential loss of privacy and how to safely share documents to other users. Understand what type data could be shared to other people: do not disclose sensitive data.</p>	<p>Lecture, practical tasks, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>

№.	Outcomes	Teaching / Learning Methods	Assessment Methods
6.14.	<p>Understand purpose of permanent data deletion from storage drives. Understand that users; deleted information could be restored from the storage drive and understand that information from the storage drives could be deleted only by IT professionals. Distinguish between deletion and permanent deletion of data from the devices. Know that external storage drives could not be thrown to the trash, know that unused storage drives and printed documents have to be destroyed. Know that unused or broken companies' storage drives or devices with storage drives, like smartphones, have to be destroyed according to companies' organisational rules.</p>	<p>Lecture, examples, recommended literature for reading and links to videos</p>	<p>Self-evaluation questions</p>
	<p><i>Summary: finished this part students have to acquire basic knowledge about workplace security. Students have to know about organisational security policy in the company, understand and know about printed documents safeguard rules in the institution, know about own devices usage in the workplace, know about company policy for installing programs and apps to the company devices, know how to use companies' devices securely, know about strong passwords creation and managing recommendations. Understand that user authorisation to devices, programs and information systems is used for identification of particular user, know about workplace ethics, know about collaboration tools and how to use them securely, understand purpose of permanent data deletion from storage drives and destruction of unused storage drives and printed documents.</i></p>	<p>Basically there should be used presentations on theoretical lectures, show videos from Youtube if there is a possibility. Practical tasks should be used for creating strong passwords and online collaboration tools usage. Discussions also could be used as a teaching method. During discussions scenarios method could be used.</p>	<p>Online test with hotspot and theoretical questions could be used for knowledge assessment. Recommendations about hotspot and theoretical questions are described in the annex.</p>

Learning outcomes for Bachelor's degree programme **Health Informatics**

Category of learning outcomes	Programme Learning Outcome	Course (module) Learning Outcome №					
		1	2	3	4	5	6
Underlying Conceptual Basis for Informatics	A1 Understanding of the key concepts and ideas of the field of information systems	√	√	√	√	√	√
	A2 Understanding of the fundamental subjects that the field of information systems requires or is based on						
	A3 Understanding of the basics of biomedicine, bioengineering, electronics, applied mathematics and other science theories						
Analysis, Design and Implementation	B1 Skills in formalization and specification of the real-world problems whose solutions involve the use of informatics						
	B2 Knowledge and skills required to model activities of enterprises and to perform detailed business analysis						
	B3 Knowledge and skills required to analyze enterprise needs, specify information systems development and modernization requirements						
	B4 Knowledge and skills required to design information systems and databases, prepare the design documentation						
	B5 Knowledge and skills in programming, testing, integrating, administrating and installing user interface, business logic and database components of information systems						
	B6 Knowledge and skills required to create multidimensional data warehouses and analyze the data stored in them						
	B7 Knowledge and skills required to plan and manage information systems' development, installation and expansion projects						
	B8 Knowledge and skills required to audit and evaluate information systems' projects as well as operational information systems						
	B9 Skills and abilities to apply information technologies (CASE tools, database managements systems, prototyping and programming environments, business modeling packages, etc.) for the solution of domain problems						

This project has been 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.

Category of learning outcomes	Programme Learning Outcome	Course (module) Learning Outcome №					
		1	2	3	4	5	6
	B10 Skills and abilities to analyze and evaluate problems related with application of information technologies and computer systems development, knowledge about new and significant informatics engineering research and development problems, and abilities to select and implement appropriate solutions for them						
	B11 Knowledge and skills to choose and apply appropriate process models and programming environments for the traditional as well as new applied informatics projects						
	B12 Skills and abilities to apply the knowledge and understanding for the formulation and solution of biomedical electronics and electronics problems, applying known methods						
Technological and Methodological Skills	C1 Skills in combining theory and practice by selecting appropriate methods and tools to solve tasks, that may arise during the development and operation of information systems						
	C2 Knowledge and skills required to plan and conduct practical research, examine experimental results						
	C3 Theoretical understanding of state-of-the-art software and hardware technologies and tools, and the skills required to use them						
	C4 Abilities and skills in domain-specific literature analysis and the recognition of the need for life-long learning						
Other Professional Competences	D1 Skills required to communicate effectively with colleagues, (potential) clients, information systems users and general public on any information systems related issues						
	D2 Skills required to systemically evaluate various tasks and situations, define their parameters, and break them down into smaller tasks at the same time providing suggestions on how to solve them						
	D3 Skills in evaluation of engineering solutions with regards to ethics, social, legal and security requirements						
	D4 Skills and abilities required to work effectively both individually and in a team, assign tasks and responsibilities, manage projects and their teams						

Category of learning outcomes	Programme Learning Outcome	Course (module) Learning Outcome №					
		1	2	3	4	5	6
	D5 Skills and abilities to understand principles of population health and their influencing factors, to evaluate health disparities and their significant social and economic factors, to identify priority health problems of the society and its groups						
	D6 Skills and abilities to understand and define the modern world, national and local health policy principles, the influence of political decisions on lifestyle and health of the population						
	D7 Skills and abilities to work in workshops and laboratories						

Summary

By taking this bended training course participants will acquire knowledge about health information systems (HIS) and about workplace IT security: Healthcare Information Systems (HIS), HIS Types, Confidentiality and security within HIS, Policy & Procedure, HIS usage, Common IT Security Knowledge, Organisational Workplace Security, Computer and Internet security.

Level of module

Level of programme		Subject group
Cycle	Degree	
First	Bachelor	Core Studies

Syllabus

№.	Sections and themes
1.	Course introduction
2.	e-services and information systems
3.	Healthcare Information Systems (HIS)
4.	HIS Types
5.	Confidentiality and security within HIS
6.	Policy & Procedure
7.	HIS usage
8.	Common IT Security Knowledge
9.	Computer and Internet security
10.	Organisational Workplace Security
11.	Course summary

Evaluation procedure of knowledge and abilities:

Ten grade and gathered evaluation system is applied. The semester's individual work tasks are evaluated by grades; the final grade is given during the examination session while multiplying particular grades by the lever coefficient and summing the products.

This project has been 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.



Erasmus+

References

№.	Title	Edition in KTU library		In KTU bookstore	Number of ex. in the methodical cabinet of the depart.
		Pressmark	Number of exemplars		
1.	Moodle e-learning platform: Health information systems and workplace IT security			No	

Additional literature

№.	Title
1.	Informacinės sistemos : vadovėlis / Leonas Simanauskas. Vilnius : VU leidykla, 2000. 292 p. : iliustr. ISBN: 9986193729. UDK: 004 (075)
2.	Informacijos sistemos ir duomenų bazės : informacijos sistemų ir reliacinių duomenų bazių kūrimo pagrindai : vadovėlis / Vitolis Sekliuckis, Saulius Gudas, Gintautas Garšva ; Kauno technologijos universitetas, Vilniaus universitetas. Technologija, 2004. 338 p. : iliustr. ISBN: 9955094869. UDK: 004.7 (075.8) ; UDK: 004.65 (075.8).
3.	Laudon, Kenneth C., 1944- Management information systems : managing the digital firm / Kenneth C. Laudon, Jane P. Laudon. 14th ed. Harlow : Pearson, 2016. 669 p. : iliustr. ISBN 9781292094007
4.	Kviklienė, Adriana. Darbo kompiuteriu pradžiamokslis vaizdžiai. 2-asis atnaujintas leid. Kaunas : Smaltija, 2011. 223 p. : iliustr. ISBN 9789955707851.
5.	Prezi mokomoji medžiaga. 2012 [dokumentas interaktyvus] prieiga internete http://prezi.com/learn/getting-started

Necessary premises, hardware and software

Lecture type	Classroom type	Places in the classroom	Required equipment / notes
Theory	Audience	30	Computer, projector, board, internet connection.
Practical lectures	Computer class	12	Computer, projector, board, internet connection.
Independent Learning	Computer class	12	Computer, projector, board, internet connection.

Lecturer

	Position	Name, surname
Coordinating	Assoc. professor	
Coordinating	Professor	
Coordinating	Lector	

This project has been 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.



Erasmus+

Subdivision

	Entitlement	Code	Contribution, %
Responsible Subdivision	Department of Software Engineering		
Another responsible Subdivision	Department of Computer Sciences		

Languages of instruction

Autumn semester:	Lithuanian, English
Spring semester:	Lithuanian

Teaching form

№	Mode of studies	Semester		Structure					Total hours	Credits
				Lectures	Practical (supervised)	Laboratory (supervised)	Tutorials	Independent Learning		
1	Standard	A	S	16	14	14	0	16	60	
2	Weekend Studies	A	S	16	14	14	0	16	60	

This project has been 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.


Erasmus+

Teaching form Standard

Schedule of individual work tasks and their influence on final grade

Skills and knowledge evaluation method	№. of syllabus	Total hours	Influence on grade, %	Week of presentment of task (*) and reporting (o)																
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17-20
Laboratory examination (introduction to HIS:1.1, 1.2, 1.7, 1.9)	1-4	2	5	*	0															
Problem-solving task	1-4	2	5	*	0															
Laboratory examination (HIS usage)	7	4	5		*	0														
Problem-solving task	7	4	5		*	0														
Laboratory examination (Common IT Security Knowledge, Computer and Internet security)	8, 9	2	5			*	0													
Problem-solving task	8, 9	2	5			*	0													
Laboratory examination (Organisational Workplace Security)	10	4	5				*	0												
Problem-solving task	10	4	5				*	0												
Examination	1-11	4	60					*	0											
Total:	-	28	100																	

Teaching form Weekend Studies

Schedule of individual work tasks and their influence on final grade

Skills and knowledge evaluation method	№. of syllabus	Total hours	Influence on grade, %	Week of presentment of task (*) and reporting (o)																
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17-20
Laboratory examination	1-11	12	20	*	0	0	0	0												
Problem-solving task	1-11	12	20	*	0	0	0	0												
Written examination	1-11	26	60						*	0										
Total:	-	28	100																	

This project has been 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.



Erasmus+