Health Information Systems training and certification implementation for higher education

Syllabus summary

Output 2
Last update: 05.06.2017
Author(s):

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.

HIS4HE syllabus summary

This syllabus provides concepts of Health information systems, policy and procedures principles, confidentiality and workplace IT security.

Who is addressed?

This syllabus is addressed for existing and future health sector professionals seeking to develop and certify their qualification in HIS usage. In the sectoral perspective, target group is health students and trainers. In labour market perspective, implementation of ECDL Health module will increase professional qualifications of young health specialists and help meet health sector requirements.

HIS4HE project cource
The project provides a blended learning course which is organised in two units (Unit 1: Health information systems, Unit 2: Worplace IT security) that are each based on different methodological concepts according to the content that is facilitated.

Syllabus summary goals

Successful participants will be able to:

- 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.

Description on the project HIS4HE

The one of objectives of this project is to support health students and existing staff working in the health sector. There is created blended learning course. Successfully finished this course participants will be prepared for ECDL e-Health and Workplace IT security tests. HIS4HE project was implemented by five partners from Lithuania, Latvia and Germany. Learning objectives in Unit 1 are derived from the ECDL / ICDL Health Information Systems Usage Version 1.5.

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+

	CATEGORY	SKILL SET	REF.	TASK ITEM
Unit 1	**1 Concepts**	*1.1 Healthcare Information Systems (HIS)*	1.1.1	Define a Healthcare Information System (HIS) as a system for holding and updating patient-related information and records, clinically as well as administratively oriented.
			1.1.2	Understand that a HIS may be made up of patient, personal or population records.
			1.1.3	Understand that electronic health records provide for history, diagnosis, documentation and management plans with respect to individual patients, and testing and procedures that result from these plans.
			1.1.4	Understand the relationship between population records and personal health records.
			1.1.5	Appreciate some of the benefits of Healthcare delivery through a HIS such as more reliable, timely information leading to better patient care.
		1.2 HIS Types	1.2.1	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.
			1.2.2	Describe 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.
			1.2.3	Identify or know about some of the functions or tools of HIS such as: booking appointments and scheduling, transmission of outputs / results, updating of patient records, giving prescriptions, home healthcare via the Internet.

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	SKILL SET	REF.	TASK ITEM
			1.2.4	Appreciate some of the potential constraints of using a HIS such as: a change in the Healthcare Professional / Patient relationship, loss of subtlety in language and data entry, loss of context of the data capture, ease of use of the patient record.
			1.2.5	Understand that a HIS supports but does not replace clinical judgment.
			1.2.6	Understand different kinds of HIS such as: office /department based, local facility based, regionally based, nationally, or internationally based.
			1.2.7	Understand the implication reliability, security, authorization to view data from your own authorized source rather than an external source.
			1.2.8	Understand different types of HIS such as: legacy / computer-based / distributed records.
	2 Due Care	*2.1Confidentiality*	2.1.1	Describe the healthcare worker's responsibilities in relation to patient confidentiality within a HIS: 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.
			2.1.2	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.
			2.1.3	Understand that local legislation gives patients the right to review and amend their own records.[1]

[1] Data Protection Act, Freedom of Information Act.

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	SKILL SET	REF.	TASK ITEM
			2.1.4	Recognise the distinction that system access does not imply authorization to view or use.
			2.1.5	Understand national requirements in terms of public reporting and management of patient specific data / rules and constraints, public health, notifiable diseases.
			2.1.6	Understand that there are certain confidentiality risks associated with HIS such as patient specific printed materials, e-mail risks.
			2.1.7	Understand that access control in a HIS is intended to protect patient's data and access to HIS is often based on: healthcare worker roles, duties and responsibilities.
		2.3 Security	2.3.1	Describe some of the key principles of security within HIS such as awareness of systems vulnerability, requirement for formal agreement to organisational security policy.
			2.3.2	Understand that an organisational security policy has personal, professional and organisational impacts.
			2.3.3	Describe some of the principal threats to a HIS such as accidental viewing, unauthorised inquiry, malicious damage, uncontrolled access, risk of transfer of data to external media.
			2.3.4	List some of the defences against security threats to a HIS.
			2.3.5	Understand the obligation to report security breaches and threats such as user impersonation, malicious attack, viruses or worms etc.
			2.3.6	Understand the concept of data storage and backup and why it is important.

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	SKILL SET	REF.	TASK ITEM
	3 HIS usage	*3.1 Navigation*	3.1.1	Understand that HIS can store patients' records as well as medical statistics.
			3.1.2	Recognise the same individual has two records created in the system, and understand authority for merging.
			3.1.3	Know how to identify the authorship of an entry in a record.
			3.1.4	Understand that there is a possibility to select and view a set of patient records based on some common criteria.
			3.1.5	Record information accurately about a patient.
			3.1.6	Know how to make the follow-up appointments/ treatment schedules for the patient.
			3.1.7	Know how to recognize different modes (automated) of data entry.
		3.2 Decision Support	3.2.1	Understand the different types of decision support that may be available such as: alerts, reminders, validation checks etc.
			3.2.2	Understand personal responsibility, authority to override system validation messages.
		3.3 Outputs Reports	3.3.1	Know how to create reports such as a patient list, a care unit census, patient bookings / appointments, theatre lists. etc.
			3.3.2	Know how to create a routine output based on a specific query such as patient results.
			3.3.3	Know how to select a type of output from a pre-existing report type/template.
			3.3.4	Know how to select and view a specific report: x-ray, ECG, CT-Scan, blood result etc.
			3.3.5	Know how to print a report securely.

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	SKILL SET	REF.	TASK ITEM
			3.3.6	Know how to transmit HIS data and reports securely.
	4 Policy & Procedure	*4.1 Principles*	4.1.1	Understand that the patient record is a legal document and no information can be erased.
			4.1.2	Understand that information can be added or amended but not changed.
			4.1.3	Understand who has the authority to create new records, e.g. Births / emergency / temporary records.
			4.1.4	Understand the audit trail within HIS and the importance thereof.

	CATEGORY	SKILL SET	REF.	TASK ITEM
Unit 2	**5 Common IT Security Knowledge**		5.1.1.	Know about advantages and disadvantages (risks) of information technologies and the internet.
			5.1.2.	Be aware about cybercrimes, financial frauds, illegal activity, viruses, hackers, avatars, spyware, keyboard spy, fraud advertisement, Trojans.
			5.1.3.	Understand the term social engineering and its implications like: unauthorised computer and device access, unauthorised information gathering, fraud. Identify methods of social engineering like: phone calls, phishing, shoulder surfing, pretenders, Spyware.
			5.1.4.	Know the term Identity; be aware about identity theft and theft methods. Be aware about spyware, keyboard spy, fraud advertisement, Trojans. Know various ways how malicious software could get into device.
			5.1.5.	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,

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	SKILL SET	REF.	TASK ITEM
				sabotage). Know about threats associated with personal data disclosure.
			5.1.6.	Know various ways how personal identity could be stolen, like phone calls, online methods (email, social network, instant messaging), skimming, shoulder surfing, information diving, deleted information recovering).
			5.1.7.	Be aware of privacy protection legal acts.
			5.1.8.	Know about organisational data management rules, data privacy principles, confidentiality.
			5.1.9.	Know to whom you may report inappropriate social network use or behavior : service provider, relevant authorities.
			5.1.10.	Understand your personal 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.)
			5.1.11.	Know about netiquette and other basic codes of conduct in the cyberspace.
	6 Organisational Workplace Security		6.1.1.	Be familiar with the organisational security policy in the company: guidelines of device usage in the workplace (know about possibility to use workplace devices for personal purposes). Know about company policy for bringing devices home.
			6.1.2.	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.
			6.1.3.	Know about company policy to bring and use own personal devices (like smartphones, tablets, USB flash drives) on the workplace. Know about company policy for connecting

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	SKILL SET	REF.	TASK ITEM
				own personal devices to the Internet and about consequences.
			6.1.4.	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) and 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).
			6.1.5.	Understand the purpose and meaning of user authorisation when he connects to the device or information system.
			6.1.6.	Identify measures for preventing unauthorised access to data like: username and password, PIN, chipcard, login using biometrical data, multi-factor authentication, one-time password. Understand that a network account should be accessed through a user name and password and locked, logged off when not in use.
			6.1.7.	Recognise ways of ensuring physical security and data theft of computers and devices like: do not leave unattended, log equipment location and details, use cable locks, access control.
			6.1.8.	Understand the importance of avoiding shoulder surfing.
			6.1.9.	Recognise safe password policies, like: adequate password length, adequate letter, number and special characters mix, not sharing passwords, changing them regularly, different passwords for different services. Understand the function, limitations of password manager.

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	SKILL SET	REF.	TASK ITEM
			6.1.10.	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.
			6.1.11.	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.
			6.1.12.	Know about periodical companies' devices revision and who performs this revision. Understand consequences if unauthorised person connects to companies' devices.
			6.1.13.	Know when and how malicious software can get into computer system. Understand the threat of malicious data spread in external data medias.
			6.1.14.	Know about workplace ethics: distinguish personal data form 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 may not be disclosed to the third parties.
			6.1.15.	Know about collaboration tools, like sharing documents on the internet to authorised persons, know about possibility to share printers and desktop to colleagues. 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.
			6.1.16.	Understand purpose of permanent data deletion from storage drives and destruction of unused storage drives and printed documents. Distinguish between deletion and permanent

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	SKILL SET	REF.	TASK ITEM
				deletion of data from the devices. Know that deleted data could be restored from storage drives. Know that unused or broken storage drives or devices with storage drives, like smartphones, have to be destroyed.
	7 Computer security		7.1.1.	Understand the importance of regularly updating software like: anti-virus, web browser, plug-in, application, operating system.
			7.1.2.	Understand how anti-virus software works and its limitations. Understand that anti-virus software should be installed on all computers and devices, and know that it is not allowed to disable antivirus in any case.
			7.1.3.	Know how to set password for documents and compressed files.
			7.1.4.	Identify main symptoms of virus infection. Know what has to be done and in what order, if you suspect that computer system is infected.
			7.1.5.	Understand the benefits and purpose of data backups. Recognise the importance of having a backup procedure in case of loss of data from computers and devices.
	8 Internet security		8.1.1.	Know how to safely browse the Internet. Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form. Be able to safely connect to e-services and secure environments. Know how to recover lost passwords.
			8.1.2.	Know about cookies, password storage on the computer or in the browser.

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	SKILL SET	REF.	TASK ITEM
			8.1.3.	Identify common characteristics of phishing like: using names of legitimate organisations, people, false web links, logos and branding, encouraging disclosure of personal information. Know who to contact if you get phishing emails. Know about dangers when opening attachments that may contain a macro or an executable file.
			8.1.4.	Be able to identify fake websites that could be opened by clicking a link from emails, on social media and etc. Know about consequences if you discover personal or companies' sensitive data on such website. Know who to contact if you discovered fake website.

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.