Sveikatos informacijos sistemos mokymų ir sertifikavimo diegimas aukštajame moksle (HIS4HE)

Programos (syllabus) santrauka

Output 2

Last update: 04.05.2018

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 programos santrauka

Ši programa apima Sveikatos informacijos sistemų sąvokas, tvarkas, procedūras, e. saugos, darbo vietos saugos, kompiuterių saugos ir konfidencialumo žinias bei įgūdžius.

Kam tai skirta?

Programa skirta aukštųjų mokymo įstaigų studentams, sveikatos informacijos sistemų naudotojams, tokiems kaip gydytojams, seselėms, slaugėms, sveikatos sistemų aptarnaujančiam personalui ir pan.
Ši programa padės įvertinti esamų sveikatos informacijos sistemų profesionalų kvalifikaciją tarptautiniu mastu Lietuvoje ir Latvijoje.
Programa remiasi Europoje pripažintu ECDL Health įgūdžių ir žinių standartu bei sertifikavimo sistema, taip užtikrinamas reikiamas žinių lygis ir kokybė.

Programos (Syllabus) santraukos tikslai

Dalyviai sėkmingai išlaikę ECDL sertifikavimo testą:

- Supras pagrindines sveikatos informacijos sistemų (HIS) savybes.
- Mokės naudoti HIS saugiai ir efektyviau.
- Supras sveikatos informacijos sistemų naudojimo etiką ir taisykles.
- Žinos apie duomenų konfidencialumą, saugą, prieigos prie duomenų valdymą naudojant HIS.
- Supras apie elektroniniu būdu įrašytus duomenis ir jų tvarkymą.
- Įgys pagrindinių žinių apie IT saugą.
- Supras darbo vietos saugą.
- Įsisąvins kompiuterių ir interneto saugos pagrindus.

Apie HIS4HE projektą

Projekto „Sveikatos informacijos sistemos mokymų ir sertifikavimo diegimas aukštajame moksle“ (HIS4HE) metu Lietuvoje ir Latvijoje siūlomi nauji mokymo standartai sveikatos studijų specialistų programai.
Projekto tikslas - parengti ir įdiegti sveikatos informacijos sistemos studijų programą, studijų modulį, mokymo medžiagą ir Europos mastu pripažintą sertifikavimo sistemą, skirtą mokymų metu įgytų žinių įvertinimui.
ECDL sveikatos informacijos sistemos sertifikavimo modulį ir priemones diegia oficialios ECDL fondo atstovybės Lietuvoje (Informacinių technologijų institutas) ir Latvijoje (LIKTA). Projekte dalyvaujantis partneris DLGI yra taip pat oficiali ECDL fondo atstovybė Vokietijoje. Šis partneris savo šalyje yra įdiegęs ECDL Health Information Systems Usage Version 1.5 (Sveikatos informacijos sistemos) modulį ir projekto HIS4HE metu dalijasi patirtimi projekto rezultatų lokalizavimo ir įdiegimo klausimais.

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.

	Kategorija	Žinių sritis	Nr.	Žinios
1 dalis	**1 Sąvokos**	*1.1 Sveikatos informacijos sistemos (HIS)*	1.1.1	Suprasti Sveikatos informacinę sistemą (HIS) kaip informacijos ir įrašų apie pacientus saugojimo ir apdorojimo sistemą, orientuotą tiek probleminiu tiek administraciniu požiūriu.
			1.1.2	Suprasti, kad HIS gali būti saugomi tiek įrašai apie konkrečius pacientus ar personalo darbuotojus, tiek apibendrinti duomenys.
			1.1.3	Suprasti, kad HIS įrašai apima tiek konkrečių pacientų diagnozes, ligos istorijas, susijusią dokumentaciją ir gydymo planus, tiek procedūras ir testus, susijusius su šiais planais.
			1.1.4	Suprasti, kaip susiję yra konkretaus asmens sveikatos įrašai ir apibendrinti įrašai apie gyventojų sveikatą.
			1.1.5	Suprasti, kad HIS teikia patikimesnę ir savalaikę informaciją sveikatos priežiūros sistemoms, tuo užtikrindama geresnę pacientų priežiūrą.
		1.2 HIS Tipai	1.2.1	Žinoti,kad HIS sudaro įvairios posistemės, pavyzdžiui, elektroniniai receptai, medicininiai vaizdai, vaistų ir laboratorinių tyrimų sistemos, sprendimų palaikymo, multimedijos, pacientų registracijos ir atsiskaitymų už paslaugas priemonės ir pan.
			1.2.2	Žinoti pagrindines HIS savybes: saugi, patikima ir greita prieiga prie duomenų įvairiais rodiniais, pastoviai atnaujinamos ir tikslios duomenų saugyklos, nuoseklūs sistemos atnaujinimo ir priežiūros procesai.

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.

	Kategorija	Žinių sritis	Nr.	Žinios
			1.2.3	Žinoti pagrindines HIS funkcijas ar įrankius, pvz., išankstinė pacientų registracija, priėmimtvarkaraštis, duomenų teikimas į susietas sistemas ar posistemius, elektroninis receptas, internetu teikiamos paslaugos, sudėtingesnės telemedicinos sistemos.
			1.2.4	Suprasti, kad IS naudojimas e-sveikatos sistemose turi ir potencialių trūkumų: keičiasi santykiai tarp sveikatos priežiūros specialistų ir pacientų, dingsta tiesioginio pokalbio ir informacijos išgavimo subtilumas, galimas konteksto praradimas.
			1.2.5	Suprasti, kad HIS yra sprendimų palaikymo, bet ne klinikinių sprendimų priėmimo sistema.
			1.2.6	Žinoti įvairius HIS tipus: skyriaus/padalinio IS, lokalus ligoninės lygis, regioninės sistemos, nacionalinės infrastruktūros, tarptautinės sistemos.
			1.2.7	Suprasti apie informacijos patikimumą, apsaugą, teises informaciją peržiūrėti lokaliame tinkle ir išoriniuose įrenginiuose.
			1.2.8	Suprasti apie įvairius HIS tipus, pvz. atgyvenusios popierinės sistemos, kompiuterinės sistemos, mišrios sistemos, paskirstyti duomenų tinklai, globalios infrastruktūros.
	2 Darbas su IS	*2.1 Konfiden-cialumas*	2.1.1	Suprasti apie sveikatos įstaigos darbuotojų atsakomybę, susijusią su pacientų HIS duomenų konfidencialumu: prieiga tik prie paciento informacijos ir tik to prireikus; prieiga tik prie operatyviai reikalingos informacijos; prieiga tik pagal turimas teises; asmeninės atskaitomybės samprata.

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.

	Kategorija	Žinių sritis	Nr.	Žinios
			2.1.2	Suprasti apie paciento teises pateikiant paciento duomenis šeimos nariams ir kitiems susietiems asmenims. Vertinti paciento teises nežinoti problemų.
			2.1.3	Suprasti vietinės juridikos klausimus apie pacientų teises peržiūrint ir keičiant savo įrašus sistemoje.[1]
			2.1.4	Suprasti skirtumą tarp prieigos prie sistemos ir autorizavimo peržiūrėti ar naudoti duomenis.
			2.1.5	Žinoti nacionalinius reikalavimus, susijusius su visuomenės informavimu apie konkrečių pacientų duomenis, žinoti apie galiojančias taisykles ir apribojimus, žinoti ligų, apie kurias būtina pranešti visuomenei, informacijos tvarkymą.
			2.1.6	Suprasti apie konfidencialumui kylančius pavojus naudojant HIS, pvz., pacientui pateikta popieriuje atspausdinta medžiaga, el. pašto naudojimo rizikos.
			2.1.7	Suprasti, kad prieigos valdymas HIS yra skirtas paciento duomenims apsaugoti ir HIS prieiga yra grindžiama sveikatos priežiūros darbuotojų rolėmis, pareigomis ir atsakomybe.
		2.3 Apsauga	2.3.1	Apibūdinti keletą pagrindinių HIS apsaugos principų: supratimas apie sistemos pažeidžiamumą, reikalavimas atitikti bendrai organizacijos saugos politikai.
			2.3.2	Suprasti apie organizacijos saugos politikos asmeninį, profesinį ir organizacinį aspektus.

[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.

	Kategorija	Žinių sritis	Nr.	Žinios
			2.3.3	Apibūdinti kai kurias pagrindines HIS grėsmes, tokias kaip atsitiktinė prieiga, nesankcionuotos užklausos, kenksminga žala, nekontroliuojama prieiga, duomenų perdavimo į išorines medias rizika
			2.3.4	Išvardinti bent kelias apsaugos nuo grėsmių sistemos saugumui priemones.
			2.3.5	Suprasti prievolę pranešti apie saugumo pažeidimus ir grėsmes, pvz., apsimetimus legaliais vartotojais, kenksmingus išpuolius, virusus ar „kirminus“ ir t.t.
			2.3.6	Suprasti duomenų saugojimo ir atsarginės kopijos sąvokas ir kodėl tai yra svarbu.
	3 **Naudojimas**	*3.1 Navigacija*	3.1.1	Suprasti, kad HIS galima saugoti tiek detalius pacientų įrašus, tiek statistinę informaciją.
			3.1.2	Suvokti, kas turi teises apjungti skirtingus įrašus apie tą patį asmenį sistemoje.
			3.1.3	Žinoti, kaip identifikuoti įrašo autorystę.
			3.1.4	Suprasti, kaip naudojant paieškos sąlygas išrinkti ir peržiūrėti klientų įrašų grupes.
			3.1.5	Mokėti taisyklingai ir patikimai suformuoti ir įrašyti įrašą apie pacientą.
			3.1.6	Mokėti priskirti paciento tolesnio gydymo paslaugas, formuoti gydymo tvarkaraštį.
			3.1.7	Mokėti naudotis įvairiais automatizuotais duomenų įvedimo būdais.
		3.2 Sprendimų palaikymas	3.2.1	Suprasti įvairias sprendimų pagrindimo ir palaikymo priemones, pavyzdžiui: perspėjimai, priminimai, užklausos patvirtinimui ir kt..

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.

	Kategorija	Žinių sritis	Nr.	Žinios
			3.2.2	Suprasti asmeninę atsakomybę, teisę nepaisyti sistemos užklausų apie patvirtinimą.
		3.3 Išvestis Ataskaitos	3.3.1	Mokėti sukurti dažniausiai naudojamas ataskaitas.
			3.3.2	Mokėti sukurti ataskaitas, pagrįstas konkrečiomis užklausomis.
			3.3.3	Mokėti pasirinkti išvesties tipą iš anksčiau sukurtų ataskaitų šablonų.
			3.3.4	Žinoti, kaip pasirinkti ir peržiūrėti specifines ataskaitas: x-ray, ECG, CT-Scan, kraujo tyrimų rezultatai ir t.t.
			3.3.5	Mokėti saugiai atspausdinti ataskaitą.
			3.3.6	Mokėti saugiai perduoti duomenis ir ataskaitas.
	4 Tvarkos ir Procedūros	*4.1 Principai*	4.1.1	Suprasti, kad paciento įrašas yra juridinis dokumentas ir jo negalima koreguoti ar pašalinti.
			4.1.2	Suprasti, kad informacija gali būti papildyta ar pakeista papildomai prijungiant, bet ne tiesiogiai keičiant.
			4.1.3	Žinoti, kas turi įgaliojimus kurti naujus įrašus, pvz., gimimo/avarijos/laikinieji įrašai.
			4.1.4	Žinoti audito seką sistemoje ir suprasti audito svarbą.

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
Dalis 2	**5 Pagrindinės e. saugos žinios**		5.1.1.	Suprasti apie informacinių technologijų, interneto galimybės ir trūkumus.
			5.1.2.	Žinoti apie kibernetinius nusikaltimus, finansines apgavystes, galimą žalą. Virusai, programišiai (hakeriai), apsimetėliai, šnipinėjimo programos (angl. spyware), šnipinėjimo įrenginiai (angl. keyboard spy), apgaulingos reklamos, Trojos arkliai.
			5.1.3.	Suprasti terminą socialinė inžinerija ir žinoti jos pasekmes: prieiga prie kompiuterių ir įrenginių be žinios; informacijos išgavimas neteisėtu būdu; lengvi laimėjimai. Žinoti socialinės inžinerijos metodus, siekiant išgauti informacijos: telefono skambučiai, sukčiavimas, žiūrėjimas per petį (angl. shoulder surfing), šnipinėjimo programos.
			5.1.4.	Suprasti tapatybės sąvoką, tapatybės vagystės būdai. Šnipinėjimo programos, nepageidaujamos reklamos, trojanai, klaviatūra renkamos informacijos rinkimas. Žinoti, kada ir kaip kenkėjiška programinė įranga gali patekti į kompiuterinę sistemą.
			5.1.5.	Suprasti tapatybės sąvoką, tapatybės vagystės būdai. Šnipinėjimo programos, nepageidaujamos reklamos, trojanai, klaviatūra renkamos informacijos rinkimas. Žinoti, kada ir kaip kenkėjiška programinė įranga gali patekti į kompiuterinę sistemą.
			5.1.6.	Žinoti apie įvairius tapatybės vagystės būdus, pavyzdžiui, skambinimas į įmonę; el. priemonių naudojimas, specialios techninės įrangos naudojimas (slaptas kopijavimas, išviliojimas, nužiūrėjimas, informacijos ieškojimas šiukšlėse, ištrintos informacijos atkūrimas – angl. *skimming, pretexting, shoulder surfing, information diving).*

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
			5.1.7.	Žinoti duomenų apsaugos teisės aktus.
			5.1.8.	Žinoti apie organizacijos duomenų tvarkymą, duomenų saugos principus, konfidencialumą.
			5.1.9.	Žinoti į ką kreiptis apie netinkamą interneto, socialinių tinklų naudojimą ir elgesį, pavyzdžiui, paslaugų teikėjai, atitinkamos institucijos.
			5.1.10.	Suprasti asmeninę atsakomybę už savo veiksmus internete: neskelbti informacijos be leidimo, būti atsakingam už savo komentarus, nesisiųsti muzikos, filmų ir kt
			5.1.11.	Žinoti apie interneto etiketą ir kitas pagrindines elgesio kibernetinėje erdvėje taisykles (RFC 1855). Žinoti apie el. laiškų rašymo etiketą, serijinių laiškų siuntinėjimą.
	6 Darbo vietos sauga		6.1.1.	Suprasti apie orgavizacinę darbo vietos saugą, įrenginių naudojimą darbo vietoje ir tvarkas išsinešti į namus, fizinę įrenginių apsaugą, jų saugojimą ir tvarkymą. svarbių spausdintų dokumentų (įskaitant slaptažodžius) palikimo be priežiūros pasekmes.
			6.1.2.	Žinoti apie spausdintų dokumentų saugojimo ir tvarkymo tvarkas. Žinoti apie svarbių spausdintų dokumentų (įskaitant slaptažodžius) palikimo be priežiūros pasekmes. Žinoti apie atsakomybę už dokumentų vagystes ir autorizuotos krepties nepaisymą.
			6.1.3.	Žinoti apie asmeninių įrenginių (išmaniųjų telefonų, planšečių, USB atmintukų) atsinešimą į darbo vietą, naudojimą, ąsmeninių įrenginių prisijungimo prie interneto galimybes, pasėkmes ir atsakomybes.

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
			6.1.4.	Žinoti apie organizacijos įrenginių (tokių kaip planšečių, išmaniųjų telefonų) naudojimo vidaus politiką (programėlių diegimą iš patikimų šaltinių, grėsmes įdiegus programėlę iš nežinomų šaltinių, įrenginių jungimą prie viešųjų interneto prieigos taškų naudojant Wi-Fi ir pan.). Žinoti apie galimas grėsmes ir pasekmes, jei į įrenginį būtų įsilaužta ar užkrėstas virusu (prieiga prie asmeninių resursų, paslėpti mokesčiai, informacijos rinkimas be žinios, vietovės nustatymas).
			6.1.5.	Žinoti saugius registravimosi kompiuteryje, išmaniajame įrenginyje būdus. Suprasti prieigos teisių prasmę ir svarbą, vartotojo asmeninę paskyrą ir kaip atskiriami skirtingų vartotojų duomenys.
			6.1.6.	Žinoti prisijungimo prie įrenginių ir sistemų apsaugos būdus, kurie leidžia išvengti neteisėtos prieigos prie duomenų: vartotojo vardas ir slaptažodžiis, PIN, lustinės kortelės, prisijungimas naudojant biometrinius duomenis, vienkartiniai slaptažodžiai, prisijungimas naudojant dvigubą patvirtinimą, vienkartinis slaptažodis. Suprasti, kad tinklo paskyra turi būti pasiekiama naudojant prisijungimo vardą ir slaptažodį, žinoti apie užrakinimo (angl. lock) ar atsijungimo (angl. log off) būdus, kai paskyra nesinaudojama.
			6.1.7.	Žinoti, kaip užtikrinti fizinę kompiuterių ir įrenginių apsaugą, kaip apsaugoti nuo duomenų vagystės, pavyzdžiui, nepalikti įrenginių (kurio paskyra yra „neužrakinta“) be priežiūros, viešai prieinamose vietose specialiu kabeliu rakinti įrenginius, užtikrinti prieigos prie įrenginių ar sistemų valdymą.

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
			6.1.8.	Suprasti, kad negalima leisti neautorizuotiems vartotojams stebėti kompiuterio ekranų (kiekvienas vartotojas privalo apsaugoti kompiuterių ekranus nuo “shoulder surfing”).
			6.1.9.	Žinoti apie saugių slaptažodžių kūrimo ir saugojimo politiką: tinkamas slaptažodžio simbolių skaičius, raidžių, skaičių ir specialių simbolių naudojimas, žinoti apie tai, kad slaptažodis turi būti reguliariai keičiamas ir niekam neatskleidžiamas, suprasti, jog skirtingoms sistemoms turi būti naudojami skirtingi slaptažodžiai. Suprasti slaptažodžių tvarkytuvės (angl. password manager) funkcijas ir ribojimus.
			6.1.10.	Suprasti, kad prisijungimo prie įrenginių, sistemų, e-paslaugų ir kitų programų vardas ir slaptažodis yra skiriamas konkretaus asmens identifikavimui ir kad šie duomenys negali būti atskleidžiami kitiems organizacijos darbuotojams. Žinoti apie pasėkmes prisijungiant kito vartotojo duomenimis.
			6.1.11.	Žinoti, kad programas darbo kompiuteryje gali diegti tik už IT ūkį atsakingi įmonės (ar IT ūkį tvarkančios išorinės įmonės) darbuotojai. Suprasti galimas grėsmes, jei prieiga prie techninės ir programinės įrangos būtų suteikta tretiesiems asmenims be leidimo.
			6.1.12.	Žinoti apie įrenginių periodinę patikrą ir kas šią patikrą atlieka.

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.

	6.1.13.	Žinoti kokiu būdu gali būti įdiegiamos šnipinėjimo programos.
	6.1.14.	Žinoti apie darbo vietos etiką: skirti asmeninę informaciją nuo verslo informacijos, žinoti kokio tipo duomenys gali būti saugomi darbo įrenginyje, suprasti apie netinkamų duomenų įrenginyje saugojimo pasekmes. Suprasti apie verslo informacijos perdavimo tretiesiems asmenims pasekmes.
	6.1.15.	Žinoti apie bendradarbiavimo programinę įrangą. Suprasti apie išteklių (rinkmenų, spausdintuvo, darbalaukio) bendrinimą ir prieigą prie jų tinkle.
	6.1.16.	Žinoti apie nereikalingų spausdintų dokumentų naikinimą, nenaudojamų įrenginių su atminties įtaisais utilizavimą (išmetamų atminties įrenginių sugadinimas mechaniniu būdu, išmagnetinimas). Suprasti dokumentų ir atminties įrenginių naikinimo esmę. Žinoti, kad ištrinti duomenys gali būti atstatyti iš atminties įrenginių.
7 Kompiuterio sauga	7.1.1.	Supasti apie nuolatinę programinės įrangos atnaujinimo svarbą: antivirusinių programų, naršyklių, programų, operacinės sistemos atnaujinimai.
	7.1.2.	Suprasti kaip veikia antivirusinės programos ir jų ribojimus. Suprasti, kad antivirusinės programos turi būti įdiegtos visuose kompiuteriuose ir išmaniuose įrenginiuose. Žinoti, jog jokiais atvejais neleidžiama išjungti antivirusinę programą.
	7.1.3.	Žinoti, kaip nustatyti slaptažodį suarchyvuotiems failams, dokumentų atidarymui ir redagavimui.
	7.1.4.	Identifikuoti pagrindinius užkrėtimo virusu simptomus. Žinoti, ką ir kuria tvarka reikia daryti, jeigu įtariate, kad kompiuteris yra užkrėstas.

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.

	7.1.5.	Suprasti duomenų atsarginių kopijų darymo tikslą ir privalumus. Suprasti apie atsarginių kopijų turėjimo svarbą praradus kompiuterį ar įrenginį (arba jiems sugedus).
8 Interneto sauga	8.1.1.	Žinoti, kaip saugiai naršyti internete. Mokėti nustatyti atitinkamus naršyklės nustatymus leidžiant arba draudžiant automatinį laukelių įrašymą (angl. autosave) užpildant formas. Gebėti saugiai prisijungti prie e. paslaugų ir saugių aplinkų, - prisijungti, naudotis, atgauti prarastus slaptažodžius.
	8.1.2.	Žinoti apie interneto slapukų privalumus, trūkumus ir pavojus, slaptažodžių išsaugojimą kompiuteryje ar naršyklėje.
	8.1.3.	Identifikuoti galimus sukčiavimo (angl. phishing) būdus: naudojant egzistuojančių organizacijų pavadinimus, žmones, netikrus svetainių adresus, skatinant atskleisti asmeninę informaciją. Žinoti ką kontaktuoti gavus apgaulingus (angl. phishing) el. laiškus. Žinoti apie pavojus, kai atveriami priedai, kuriuose gali būti makrokomandos ar vykdomasis failas.
	8.1.4.	Sugebėti identifikuoti netikras svetaines, kurios gali būti atvertos paspaudus nuorodas, esančias elektroniniuose laiškuose, socialiniuose tinkluose ir kt. Žinoti apie pasekmes, jeigu atskleisite jautrius asmens arba organizacijos duomenis tokiose svetainėse. Žinoti, į ką kreiptis, jeigu aptikote tokią netikrą svetainę.

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.