

Corso ECM

Nome Provider: Cosmopolis società Cooperativa Id. 584

Titolo: L'informatica per le professioni sanitarie – Sanità digitale

Edizione: 1°

Sede: Catania, Via del Bosco n. 267/b

Destinatari: 10

Obiettivi formativi: argomenti di carattere generale: informatica e lingua inglese scientifica di livello avanzato. normativa in materia sanitaria : i principi etici e civili del ssn

Area Formativa: per tutte le professioni

Data/e: 24-29-31 Maggio 2017

Responsabile Scientifico: VIRDI ANDREA RICCARDO

CREDITI assegnati: 23,2

PROGRAMMA:

Docente Saitta Rosa Maria Samuela (eventuale sostituto Viridi Andrea Riccardo)

Giorno	Orario	Metodologia	Descrizione
24/05/17	15:00 – 18:30	Didattica frontale – lezione magistrale	Informatica di base ed internet
24/05/17	18:30 – 20:30	Didattica attiva- Esecuzione diretta da parte di tutti i partecipanti di attività pratiche o tecniche	Sicurezza informatica e Privacy dei dati sanitari
29/05/17	15:00 – 16:30	Didattica frontale – lezione magistrale	Documenti informatici-firma digitale, archiviazione. Codice della Amministrazione Digitale
29/05/17	16:30 – 18:30	Didattica attiva- Esecuzione diretta da parte di tutti i partecipanti di attività pratiche o tecniche	Digitalizzazione e archiviazione documentale.
29/05/17	18:30 – 20:30	Didattica attiva- Esecuzione diretta da parte di tutti i partecipanti di attività pratiche o tecniche	Protezione elettronica del dato personale.
31/05/17	15:00 – 18:00	Didattica frontale – lezione magistrale	Introduzione alla telemedicina. Gli strumenti del web 2.0: le tecnologie di

			aggregazione, collaborazione e scambio al servizio di medici e pazienti
31/05/17	18:00 – 20:00	Didattica attiva- Esecuzione diretta da parte di tutti i partecipanti di attività pratiche o tecniche	E-Health: Soluzioni ed applicazioni digitali in ambito sanitario
31/05/17	20:00 – 21:00		Conclusione ed esame orale.

Segreteria scientifica:
Segreteria organizzativa:

Virdi Andrea Riccardo
Saitta Rosa Maria Samuela
Via Roma, 353
Enna, 94100 (EN)
+39 0935 1830135, info@learningconnections.it

Razionale

Con il termine E-health, di recente ideazione, si fa riferimento all'utilizzo di strumenti informatici, personale specializzato e tecniche di comunicazione medico-paziente nella pratica della salute, e quindi al complesso delle risorse, soluzioni e tecnologie informatiche di rete applicate alla salute ed alla sanità.

Con la crescente diffusione ed applicazione di soluzioni ICT (Information & Communications Technology) nel settore della sanità, si rende necessario salvaguardare la sicurezza informatica e la privacy del cittadino-utente e paziente, sempre più coinvolto nei nuovi processi di profilazione e gestione dei dati personali e sensibili. La sempre maggiore integrazione dei processi amministrativi, organizzativi e clinici tra le diverse strutture sanitarie e l'avvio di reti regionali sanitarie a supporto di modelli organizzativi innovativi, che promuovono la continuità delle cure e la centralità del servizio al cittadino, generano il bisogno di valide garanzie di sicurezza, per gli utenti come anche per chi gestisce questa enorme mole di dati personali.

Rispettare le normative vigenti e tutelare le informazioni personali dei cittadini-utenti del servizio, vuol dire oggi gestire il settore sanitario curando l'informatizzazione con particolare riguardo alla gestione della sicurezza delle informazioni trattate.

Il Codice della privacy dedica al trattamento dei dati personali in ambito sanitario l'intero titolo V della parte II, e precisamente dall'art. 75 all'art. 94.

In linea generale, la sicurezza di un sistema informatico dipende non solo da aspetti tecnici, ma anche e soprattutto da quelli organizzativi, questi ultimi traducibili nella:

- Definizione di Politiche di sicurezza e protezione delle risorse informatiche, tanto fisiche (hardware) quanto logico-funzionali (software);
- Attuazione delle Politiche così definite, attraverso l'individuazione dei beni da proteggere e delle minacce a cui i detti beni sono sottoposti, la mappatura dei rischi,
- l'analisi dei costi/benefici; l'implementazione del sistema di sicurezza;
- l'aggiornamento e manutenzione; la formazione del personale dirigenziale ed operativo;
- Verifica della corretta attuazione e della efficienza delle misure adottate (Audit di sicurezza).

Da un punto di vista implementativo, è necessario che ogni struttura dotata di Sistemi Informativi automatizzati definisca un Piano di Sicurezza, in grado di fornire servizi secondo standard di riservatezza nell'accesso ai dati (prevedendo per es. meccanismi di autenticazione forte come i dispositivi biometrici, le password dinamiche, i certificati digitali, ecc..), disponibilità (ovvero di fruibilità delle risorse da parte dell'utente autorizzato in presenza di guasti informatici o di eventi catastrofici) in una logica di business continuità, integrità delle informazioni-comunicazioni (in tale contesto l'adozione della firma elettronica, nelle sue declinazioni avanzata, qualificata e digitale, e del processo di conservazione digitale, rafforzano il tema dell'integrità, affermando i principi di autenticità

e certezza dell'origine del documento oggetto di firma digitale), autenticità (ovvero certezza sulla provenienza dei dati racchiusi nel messaggio), affidabilità.

Nel quadro dei più generali obblighi di sicurezza, i titolari del trattamento sono tenuti ad assicurare un livello minimo di protezione dei dati personali che, ove trattati con strumenti elettronici, si traduce concretamente nell'obbligo di:

- adottare un Sistema di autenticazione informatica;
- ricorrere a Procedure di gestione delle credenziali di autenticazione;
- adottare un Sistema di autorizzazione;
- aggiornare periodicamente l'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- proteggere gli strumenti elettronici e i dati da trattamenti illeciti di dati, da accessi non consentiti a determinati programmi informatici;
- adottare procedure per la custodia di copie di sicurezza, per il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- utilizzare tecniche di cifratura o codici identificativi, per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

I contenuti del corso possono essere suddivisi in cinque moduli didattici:

Modulo 1: Informatica di base ed internet

Modulo 2: Digitalizzazione e archiviazione documentale

Modulo 3: Protezione elettronica del dato personale

Modulo 4: Sicurezza informatica e Privacy dei dati sanitari

Modulo 5: E-Health: Soluzioni ed applicazioni digitali in ambito sanitario

La trattazione degli argomenti "Sanità Digitale" non può prescindere dalla trattazione dei concetti basilari dell'informatica e dalla illustrazione delle principali regole di funzionamento del computer (Modulo 1).

Il Modulo 2 è dedicato al processo di dematerializzazione del documento cartaceo, di conservazione sostitutiva ed archiviazione digitale del medesimo, con una finestra sulle principali tecniche di firma digitale del documento informatico.

Il Modulo 3, invece, introduce il candidato ai concetti di Privacy, di protezione del dato personale e di misure di sicurezza. Con la crescente diffusione ed applicazione di soluzioni ICT (Information & Communications Technology) nel settore della sanità, si è dunque resa necessaria l'adozione di accorgimenti a tutela della sicurezza informatica e della privacy del cittadino-utente-paziente, sempre più coinvolto nei nuovi processi di profilazione e gestione dei dati personali e sensibili: il Modulo 4 illustra nel dettaglio le regole prescritte dal Codice della Privacy in materia di trattamento dei dati personali sanitari e di misure di sicurezza a tutela della riservatezza ed integrità dei dati stessi. Il generale principio sancito dal Codice dell'amministrazione digitale (o CAD), secondo cui le Pubbliche

amministrazioni sono chiamate ad assicurare “disponibilità, gestione, accesso, trasmissione, conservazione e fruibilità dell'informazione in modalità digitale”, ha così trovato applicazione concreta anche nel settore della sanità: il Modulo 5 ripercorre l'iter di sviluppo del concetto di "sanità in rete", analizzando le principali soluzioni applicative della sanità elettronica (o eHealth) attualmente in fase di progettazione o sperimentazione presso le varie strutture sanitarie del territorio nazionale o regionale.

Gli iscritti al corso alterneranno esperienze di lezioni frontali con esercitazioni pratiche di laboratorio utilizzando le risorse hardware e software disponibili nella sede di svolgimento dell'evento.

Sono previsti nr. tre incontri ; a conclusione del monte orario complessivo dell'evento verranno eseguite le prove di verifica obbligatorie, attraverso la prova orale.

Ai corsisti verrà assegnata una Ei-card Eipass per accedere ai contenuti didattici online ed alla piattaforma di certificazione Didasko, messa a disposizione nella sede di svolgimento dell'evento, in qualità di Ei-center Eipass accreditato, con il rilascio della relativa certificazione EiPass Sanità Digitale.

Il modello didattico assume quindi anche una connotazione post-formativa permettendo ai corsisti di accedere al materiale didattico da remoto anche successivamente alla conclusione del corso, qualora ritenessero opportuni approfondimenti.