PROGETTO FORMATIVO AZIENDALE

TITOLO DEL CORSO	Tutela della privacy. Open data e tutela dei dati sanitari
NUMERO PARTECIPANTI	20
DESTINATARI (qualifica)	Tutti i professionisti della salute
ARTICOLAZIONE CORSO	2 incontri di 3 ore ciascuno
TOTALE ORE	6
NUMERO EDIZIONI	1
DATA	16 e 22 giugno
ORARIO	09.00-12.00
AULA	CRAL
RESPONSABILE SCIENTIFICO DEL CORSO	Dr. Natale Lo Castro
DOCENTI	Dr. Natale Lo Castro, Ing. Guglielmo Toscano, Dr. Alessandro Coccia

OBIETTIVO GENERALE:	Aggiornare le conoscenze dei partecipanti sulle tematiche della tutela della privacy in ambito sanitario connettendole alle esigenze della trasparenza amministrativa secondo il "Piano di cresita digitale" previsto dal governo.
OBIETTIVI SPECIFICI:	• comprendere ed applicare le misure di sicurezza per la raccolta ed il trattamento dei dati sanitari • identificare le responsabilità del Responsabili ed Incaricati per la salvaguardia della privacy

METODOLOGIA DIDATTICA:

- **A.** Lettura magistrale
- **B.** Relazione predefinita
- **C.** Tavole rotonde con dibattito tra esperti
- **D.** Confronto/dibattito tra pubblico ed esperto/i guidato da un conduttore
- **E.** Dimostrazioni tecniche senza esecuzione diretta da parte dei partecipanti
- **F.** Presentazione di problemi/casi clinici in seduta plenaria (non a piccoli gruppi)
- **G.** Lavoro a piccoli gruppi su problemi/casi clinici con produzione di rapporto finale
- **H.** Esecuzione diretta di tutti i partecipanti di attività pratiche o tecniche
- **I.** Role playing

PROGRAMMA

1° INCONTRO - 9.00-12.00

9.00 - 10.00

Titolo: Introduzione agli OpenData – Il principio di trasparenza

10.00 - 11.00

Titolo: Gli Open data e le prospettive prioritarie del miglioramento delle performance della PA e delle ricadute positive in ambito assistenziale

11.00 - 12.00

Titolo: Il delicato ruolo dell'operatore sanitario nella salvaguardia della riservatezza del cittadino nel percorso di cura

DOCENTI/SOSTITUTI: Natale Lo Castro,Guglielmo Toscano, Alessandro Coccia

2° INCONTRO - 9.00-12.00

9.00 - 10.00

Titolo: Misure di sicurezza generale dei sistemi di elaborazione dati aziendali

10.00 - 11.00

Titolo: Misure pratiche attuative delle misure di sicurezza in azienda

11.00 - 12.00

Titolo: Utilizzo di: antivirus, antispam, firewall, modalità d'accesso alle banche dati, casi pratici di attuazione delle misure in azienda

DOCENTI/SOSTITUTI: Natale Lo Castro,Guglielmo Toscano, Alessandro Coccia.

ore 12,00-12.30 Test di verifica

ABSTRACT

I dati aperti, comunemente chiamati con il termine inglese **open data** anche nel contesto italiano, sono dati liberamente accessibili a tutti le cui eventuali restrizioni sono l'obbligo di citare la fonte o di mantenere la banca dati sempre aperta. L'open data si richiama alla più ampia disciplina dell'open government, cioè una dottrina in base alla quale la pubblica amministrazione dovrebbe essere aperta ai cittadini, tanto in termini di trasparenza quanto di partecipazione diretta al processo decisionale, anche attraverso il ricorso alle nuove tecnologie dell'informazione e della comunicazione.
Il Decreto legislativo 196/2003 in materia di protezione dei dati personali introduce regole precise relative al trattamento dei dati personali per garantire correttezza, integrità ed aggiornamento delle informazioni. Le misure di sicurezze obbligatorie per legge e quelle opportune per proteggere i dati personali da intrusioni esterne saranno rivisitate in modo sistematico con i partecipanti al corso, in particolar modo per quanto attiene ai dati definiti sensibili. Saranno quindi analiticamente analizzati i compiti dei responsabili e degli incaricati del trattamento dei dati. I diritti del cittadino/utente relativamente al trattamento dei propri dati personali costituisce una parte importante della normativa sulla privacy, che sarà trattata in questo incontro. Il consenso al trattamento dei dati, le modalità di accesso alla documentazione sanitaria, le misure per il rispetto della riservatezza degli interessati, le norme deontologiche ed il segreto professionale saranno rivisitati e discussi con i partecipanti e contestualizzati nelle specifiche realtà lavorative.
Il Rapporto tra riservatezza ed accesso ai dati di natura sensibile – il problema del bilanciamento > Il diritto all'informazione e quello alla *privacy* costituiscono due interessi di rango primario che, in quanto tali, devono ritenersi entrambi meritevoli di costante ed adeguata tutela da parte dell'ordinamento giuridico. Il primo si realizza attraverso l'esercizio del diritto di accesso alla documentazione amministrativa e si basa sull'esigenza di trasparenza ed imparzialità dell'azione amministrativa; il diritto alla riservatezza dei soggetti terzi, invece, inerisce alla sfera degli assetti privatistici e si traduce nella necessità di garantire la segretezza dei c.d. dati sensibili, quali risultano individuati e definiti dal legislatore nella normativa di riferimento, che specificamente contiene la disciplina della protezione dei dati personali.
La documentazione sanitaria criticità e responsabilità penali e civili della corretta tenuta del documento sanitario > IL D.Lgs.vo n. 196/03 "Codice in materia di protezione dei dati personali" contempla diverse disposizioni che apprestano tutela al diritto al controllo esclusivo dei propri dati personali sul piano amministrativo, civile e penale. In materia di responsabilità civile (art. 15 Codice) il codice riconduce la responsabilità stessa a quella prevista dall' art. 2050 del c. c. equiparando il trattamento di dati personali ad " attività pericolosa" . La responsabilità in campo penale,invece, è disciplinata dall' art. 169 del Codice , il quale sanziona la mancata adozione , da parte di chi vi è tenuto , delle misure minime di sicurezza dicui all' art. 33 del Codice stesso.
Il principio di necessità ed il principio di pertinenza e non eccedenza nel trattamento dei dati personali di natura sensibile > L'art. 3 introduce il "principio di necessità" nel trattamento deidati personali, in base al quale, sin dalla loro configurazione, i sistemi informativi ed i software devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità consentite, e non anche quando i medesimi obiettivi possano essere raggiunti mediante l'uso di dati anonimi o che comunque consentano una più circoscritta identificazione degli interessati. Il principio introdotto integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati.