european informatics passport

Programma analitico d'esame

SANITÀ DIGITALE

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Informatica di base e www

Il modulo intende accertare nel candidato il possesso delle competenze digitali relative sia ai fondamenti dell'hardware, posti alla base dell'Information Technology, che all'utilizzo delle più comuni funzioni di un Sistema Operativo ad interfaccia grafica, con particolare attenzione alla gestione ed alla organizzazione dei file e delle cartelle.

In particolare, il candidato dovrà mostrarsi in grado di:

- Descrivere i concetti generali della Tecnologia dell'Informazione;
- Classificare i computer;
- Descrivere la principali componenti costituenti un computer;
- Descrivere le periferiche di input e di output;
- Descrivere le varie tipologie di memoria e di dispositivi per la memorizzazione;
- Gestire adeguatamente le risorse laboratoriali;
- Misurare le informazioni utilizzando le più comuni unità di misura;
- Descrivere ed applicare all'utilizzo pratico i concetti generali per la gestione di un sistema operativo ad interfaccia grafica (GUI);
- Installare e disinstallare un programma applicativo;
- Gestire autonomamente file e cartelle.

Secondariamente, si certificano le competenze possedute in ordine all'utilizzo di servizi di rete.

In particolare, il candidato dovrà mostrarsi in grado di:

- Utilizzare un Browser per la navigazione in rete
- Utilizzare efficacemente un motore di ricerca
- Utilizzare servizi di posta elettronica
- Utilizzare aree riservate per la condivisione e la trasmissione di dati e documenti

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
Conoscere i concetti generali della Tecnologia dell'Informazione	Analisi di base componenti hardware	a. Indicare la corretta accezione di base del termine "hardware" b. Indicare i principali componenti hardware di un computer
	Classificazione dei computer	a. Descrivere un computer, definendo le differenze caratterizzanti le varie tipologie disponibili (PC, notebook, laptop, smartphone, mainframe, ecc.)
	Analisi e gestione dei dispositivi di memoria	a. Distinguere e denominare i diversi tipi di memoria centrale presenti nel computer (RAM, ROM, EPROM, CACHE) in relazione alla loro tipologia e funzione b. Riconoscere i principali tipi di dispositivi di archiviazione (memorie di massa), quali: CD, DVD, "pendrive", dischi fissi, archivi remoti, unità di rete
	Porte di input/output	a. Descrivere caratteristiche e differenze fra le porte di input disponibili su un computer (USB, seriale, parallela) b. Descrivere caratteristiche e differenze fra le porte di output disponibili su un computer (VGA, audio, ecc.)

	Le periferiche di Input/Output	a. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di output b. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di output c. Data una serie di periferiche, individuare quelle deputate a svolgere funzioni di sia di input che di output
Ottimizzare le risorse	Gestione delle risorse	a. Classificare le risorse di laboratorio in base alle caratteristiche delle stesse b. Individuare ed applicare i migliori criteri di ergonomia c. Individuare corretti principi di condivisione delle risorse disponibili in base ai vari possibili contesti operativi
Comprendere i concetti generali per la gestione di un sistema operativo ad interfaccia grafica	Impostazione e personalizzazione di un Sistema Operativo ad interfaccia grafica	a. Descrivere le principali procedure per modificare la configurazione dell'interfaccia grafica e delle impostazioni di "default" (impostazioni audio, impostazioni risoluzioni schermo, ecc.) b. Indicare la corretta procedura di installazione di un "software applicativo" c. Indicare la corretta procedura di disinstallazione di un "software applicativo"

Comprendere le modalità e le funzionalità di gestione di file e cartelle	Concettualizzazione di base	a. Indicare e denominare i supporti hardware utili alla archiviazione di file e cartelle b. Indicare come un Sistema Operativo ad interfaccia grafica (GUI) visualizza le unità disco, le cartelle, i file e la struttura nidificata di questi ultimi (funzione dei segni + e – accanto alle cartelle) c. Descrivere e differenziare le più diffuse modalità di misurazione dei file e delle cartelle (KByte, MByte, GByte) d. Indicare la procedura utile alla creazione di copie di backup di file e cartelle su dispositivi remoti; viceversa, indicare le modalità di ripristino di copie di backup precedentemente create
	Gestione di cartelle	a. Creare, eliminare, denominare e rinominare, aprire, chiudere, comprimere una cartella b. Organizzare il contenuto di una cartella secondo criteri differenti c. Accedere alle proprietà di una cartella per analizzarle e modificarle

	Gestione di file	a. Indicare l'uso dell'estensione di un file, e riconoscere in base alla loro estensione i file di tipo più comune b. Archiviare un file attribuendogli un nome, una destinazione, un formato c. Rinominare un file precedentemente creato d. Modificare l'ordine dei file visualizzati in una cartella, scegliendo tra le opzioni disponibili e. Dalle proprietà di un file, riconoscere e possibilmente modificare le sue impostazioni sorgenti
Utilizzare un Browser per la navigazione in rete	Definire caratteristiche e funzionalità del Browser	a. Definire cosa è un Browser b. Discriminare funzioni e strumenti impiegabili in un Browser c. Orientarsi fra le opzioni disponibili per la gestione del Browser

Utilizzare un Browser	a. Impostare la pagina iniziale del Browser utilizzando le opzioni disponibili b. Gestire le funzioni di cronologia delle esplorazioni c. Gestire le funzioni di eliminazione d. Gestire le funzioni di protezione e. Modificare opportunamente le impostazioni di visualizzazione f. Modificare la barra strumenti del Browser g. Chiudere una scheda/tutte le schede precedentemente aperte h. Gestire le preferenze i. Gestire le opzioni di visualizzazione j. Gestire la barra strumenti k. Impostare un criterio di protezione

Utilizzare efficacemente un motore di ricerca	Gestire le funzioni di un motore di ricerca	a. Definire il concetto di indicizzazione b. Ricercare un argomento di interesse utilizzando parole, simboli, stringhe frasali a seconda dei casi c. Salvare pagine contenenti le informazioni desiderate d. Traslare, quando possibile, il contenuto di pagine in documenti di testo e. Utilizzare un motore di ricerca per il reperimento di immagini f. Utilizzare un motore di ricerca per il reperimento di eventi g. Utilizzare funzioni di traduzione contestuali al motore di ricerca h. Utilizzare opportune protezioni nei confronti di siti non certificati i. Bloccare siti non adeguati all'Utenza
Utilizzare servizi di posta elettronica	Caratteristiche e funzionalità dei servizi di posta elettronica	a. Definire cosa è un Client b. Definire cosa è un Account c. Definire cosa è un Server di Posta elettronica d. Definire i concetti di Userid e Password e. Discriminare le caratteristiche dei servizi di posta elettronica rispetto a quelle di altri servizi di comunicazione in rete

	Utilizzare un servizio di posta elettronica	a. Impostare un account di posta elettronica in base a criteri di invio e ricezione messaggi b. Impostare un client di posta elettronica c. Impostare correttamente le opzioni di invio e ricezione rese disponibili dal client o dal server impiegato d. Impostare un criterio di priorità e. Impostare un criterio di invio f. Impostare un criterio di lettura del messaggio da parte del destinatario g. Allegare al messaggio un file, una cartella h. Ricercare un messaggio all'interno della posta inviata o ricevuta i. Impostare un elenco di posta indesiderata j. Bloccare un mittente k. Impostare un criterio di protezione alla posta ricevuta l. Discriminare messaggi di posta elettronica pericolosi per la propria privacy
Utilizzare aree riservate per la condivisione e la trasmissione di dati e documenti	Accedere ad un'area riservata	a. Registrarsi in un'area riservata b. Identificarsi in un'area riservata c. Modificare i dati relativi all'Account Utente d. Effettuare il download di documenti

Documento informatico, conservazione sostitutiva ed archiviazione, firme elettroniche

Il modulo intende accertare nel candidato il possesso di competenze relative alle modalità di archiviazione dei documenti digitali e alla disciplina legata alla pratica di conservazione dei documenti elettronici. In successione saranno affrontate le tematiche relative alla dematerializzazione degli archivi informatici, alle copie digitali dei documenti e in generale alla conservazione degli stessi.

Ogni aspetto sarà considerato sempre facendo riferimento al quadro normativo più aggiornato, l'azione di verifica valuterà la comprensione anche di quest'ultimo, insieme all'acquisizione particolareggiata delle pratiche e degli elementi normativi che riguardano la firma digitale ed elettronica.

In particolare, il candidato dovrà mostrare la propria preparazione in ordine ai seguenti argomenti:

- Digitalizzazione e archiviazione documentale
- Dematerializzazione degli archivi
- Disciplina probatoria dei documenti elettronici
- Copie digitali
- Conservazione dei documenti elettronici
- Firme elettroniche e digitali

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
Digitalizzazione e archiviazione documentale	L'archivio e i flussi documentali	a. Concetto di archivio b. Classificazione c. Fascicolo d. Flussi documentali
	Gli "oggetti" dell'archivio digitale	a. Regole per l'archiviazione e conservazione dei documenti in formato digitale b. Documenti analogici obbligatori
Documenti informatici	La dematerializzazione degli archivi	a. Definizioni introdotte dal Codice dell'Amministrazione Digitale (CAD)
	La disciplina probatoria dei documenti informatici	a. Validità dei documenti informatici b. Apposizione di firma digitale
	Le copie	a. Art. 22 del CAD b. Copie di documenti informatici e loro validità c. Procedure di validazione
Conservazione dei documenti informatici	Il sistema e i requisiti per la conservazione	a. Caratteristiche del sistema di conservazione b. Differenza tra sistema analogico e sistema digitale di conservazione c. Formati di conservazione d. Pacchetti informativi e. Soggetti coinvolti nel sistema di conservazione
	Il Responsabile della conservazione	a. Funzioni b. Conformità del processo

	Il Manuale della conservazione	a. Elementi essenziali b. Fasi del processo di conservazione sostitutiva
	Nuove regole tecniche per i sistemi di conservazione	a. Regime transitorio
Firma elettronica	Evoluzione	a. Introduzione b. Primi certificatori accreditati c. Gli organi di vigilanza
	La situazione giuridica oggi	a. Codice civile e firma elettronica b. Efficacia della scrittura privata c. Sottoscrizione autenticata d. Copie di atti pubblici e scritture private e. Codice penale e firma elettronica
	Le firme elettroniche nell'Unione Europea	a. Direttive comunitarie b. Divergenze con la normativa nazionale c. Le Decisioni più recenti
	Legislazione nazionale	a. Tipologie definite dal CAD
	Firma elettronica	a. Firme elettroniche non verificabili b. SSCD c. Firma elettronica avanzata
	Firma digitale	a. Definizione b. Caratteristiche c. Firma elettronica qualificata

Differenza tra firma digitale e firma elettronica qualificata	a. Certificato qualificato b. Crittografia asimmetrica c. Controllo esclusivo del dispositivo di firma d. Dispositivo sicuro per la generazione della firma e. Requisiti per i dispositivi sicuri per la generazione della firma elettronica qualificata f. Requisiti dei dispositivi per la generazione della firma digitale
Base tecnologica	a. Crittografia b. Crittografia e firma digitale
Processo di generazione	a. Fasi della generazione di una firma digitale
Verifica della firma digitale	a. Fasi del processo di verifica

Protezione elettronica del dato personale

Il modulo intende fornire al candidato le necessarie competenze per occuparsi della gestione dei dati personali senza violare le normative sulla privacy e affrontare in modo adeguato le problematiche legate al tema della sicurezza informatica. Il punto di partenza è il Codice per la protezione dei dati personali che trova fondamento nella Carta dei diritti fondamentali dell'Unione europea in cui si colloca il diritto alla riservatezza o privacy. In esso si stabilisce che i dati personali siano trattati solo dietro esplicito consenso; un diritto che afferma la libertà e la dignità della persona, preservandola da quello che può essere definito "potere informatico".

Le nuove tecnologie digitali pongono infatti numerosi interrogativi rispetto alla privacy, in quanto l'utilizzo dei servizi internet, della mail o degli acquisti su internet, e naturalmente anche i rapporti con la PA digitale richiedono continuamente il trattamento dei dati personali che non può essere lasciato ad un uso privo di limitazioni e procedimenti definiti e condivisi.

L'avvento del web 2.0 ha reso ancor più urgente la regolamentazione della privacy e le normative sulla sicurezza informatica in quanto ha reso ancora più diffusa e frequente la pratica della comunicazione sul web con la condivisione di file multimediali di ogni tipologia: dalle foto, ai video, ai messaggi testuali o audio.

Nella trattazione presente nel modulo 5 troverà spazio la normativa sul Garante della privacy e quella relativa ai diritti dell'interessato e alle modalità di fornire il consenso.

Qui in dettaglio gli aspetti affrontati nel modulo:

- Privacy: definizione ed evoluzione
- Codice in materia di protezione dei dati personali
- I diritti dell'interessato
- Le regole in materia di protezione dei dati personali
- Le regole specifiche dei soggetti pubblici
- Privacy e diritto di accesso
- Le misure di sicurezza
- Il *disaster recovery*

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
Privacy: definizione ed evoluzione	Privacy come diritto alla riservatezza	a. Origini b. Carta dei diritti fondamentali dell'Unione europea
	Nuova dimensione della Privacy	a. Incremento dei dati scambiati b. Necessità di accordi internazionali c. Rischi d. D.L. n.196 del 30.06.2003
Codice in materia di protezione dei dati personali	Caratteristiche principali	a. Le suddivisioni principali b. La definizione di dato personale e comunicazione c. Ambito di applicazione del Codice d. Finalità e necessità del trattamento dei dati personali
	Figure connesse alla protezione dei dati personali	a. Il garante b. Il titolare c. L'interessato d. Il responsabile e. L'incaricato
I diritti dell'interessato		a. Diritto a ottenere informazioni sul trattamento dei propri dati b. Diritto alla modifica e alla cancellazione dei propri dati.
Le regole in materia di protezione dei dati personali	Limiti e obbligazioni delle P.A. in merito al trattamento dati	a. Individuare gli attori coinvolti b. Art.5 della Convenzione di Strasburgo c. La Direttiva Europea 95/46/CE
	Criticità	a. Responsabilità civile b. Danni e risarcimenti c. Cessazione del trattamento

Le regole specifiche per i soggetti pubblici	Comunicazioni e accessi	a. Limiti e obblighi della PA relativi al trattamento dati dei suoi utenti b. D.P.R. 14 novembre 2002, n. 313
	Dati sensibili	a. Normativa b. Autorizzazioni c. Raccomandazioni del Garante
	Banche dati	a. Visibilità e riservatezza b. Big data c. Open data
Privacy e diritto di accesso	Esigenze in conflitto: trasparenza e imparzialità contro riservatezza	a. Diritto di accesso b. Condizioni in cui il diritto alla privacy non risulta prioritario
Il consenso al trattamento dei dati personali	Consenso in forma scritta	a. Art.23 Codice della Privacy
	Validità e modalità del consenso	a. Esplicitazione delle modalità di utilizzo dati b. Casi in cui il trattamento dati è consentito anche in assenza di esplicito consenso
Le misure di sicurezza	Adozione misure per la protezione dati	a. Art.34 del Codice Privacy b. Art.35 del Codice Privacy c. Misure minime
	Aggiornamento periodico e controllo	a. Novità in materia di sicurezza nel Codice della Privacy b. Decreto semplificazioni c. Reato di frode informatica

	Documento programmatico sulla sicurezza e misure minime	a. Strumenti di autenticazione b. Procedure di aggiornamento c. Sistemi di autorizzazione e protezione da accessi non autorizzati d. Adozione di procedure di backup e. Obbligo di adozione di protezioni crittografiche f. Documento programmatico sulla sicurezza
Il disaster recovery	Continuità operativa	a. Cause: malfunzionamenti, attacchi esterni, virus b. Priorità applicative c. Protezioni: backup dei dati, ridondanza dei dati, software anti-virus, gruppi di continuità, firewall, centri data alternativi.

Sicurezza informatica e Privacy dei dati sanitari

Per superare questo modulo, il candidato deve dimostrare di conosce gli strumenti di identificazione in rete e le tecniche di comunicazione in sicurezza tra gli interlocutori, capaci di rendere le informazioni indecifrabili, in modo che solo il mittente e il destinatario possano leggerle, assicurandone l'integrità e consentendo l'autenticazione dei soggetti coinvolti. La crittografia, in tal senso, si propone di ricercare algoritmi capaci di proteggere, con un considerevole grado di sicurezza, le informazioni da possibili attacchi criminali, della concorrenza o di chiunque possa usarle per arrecare danno: essa comprende tutti gli aspetti relativi alla sicurezza dei messaggi, all'autenticazione degli interlocutori, alla verifica dell'integrità. Servizi di recente sperimentazione all'interno delle strutture sanitarie, come la refertazione on-line, il Fascicolo sanitario elettronico (Fse) e/o il Dossier sanitario, obbligano i titolari del trattamento a predisporre e adottare misure minime di sicurezza, dunque specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (per esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).

In sostanza, conformemente con quanto prescritto dal Codice della privacy, devono essere assicurati:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (per esempio, in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale, dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Il Candidato deve comprendere che la protezione dei dati digitali in ambito sanitario, è conseguibile attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurarne:

- l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
- la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
- la correttezza dei dati (integrità);
- l'oscuramento dei dati (cifratura);
- la protezione del sistema da attacchi di software malevoli.

Il Modulo approfondisce i contenuti più importanti in tema di sicurezza informatica e privacy nel contesto sanitario, in modo tale che il Candidato deve dimostrare di conoscere:

- le regole e i principi, generali e particolari, in fatto di trattamento dei dati idonei a rivelare lo stato di salute del paziente, di accesso ai medesimi, di obblighi e misure di sicurezza a tutela dei diritti e libertà fondamentali, della dignità dell'interessato, con particolare riferimento alla riservatezza;

- l'intima connessione esistente tra i citati concetti, dato che solo un sistema in grado di proteggere i dati personali e/o sensibili, riesce a fornire uno strumento sicuro agli operatori e ai fruitori in generale del servizio informatico;
- e far proprio il principio per cui il continuo aggiornamento professionale, unito alla consapevolezza dell'importanza delle norme di settore, sono gli strumenti più efficaci per far fronte ai problemi della sicurezza informatica.

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
Sintesi dei principi e delle regole generali in materia di protezione dei dati personali	Contenuto dei diritti e liberta fondamentali del soggetto interessato	a. conoscenza dei presupposti e delle modalità per un trattamento dei dati personali che salvaguardi diritti, libertà fondamentali e dignità dell'interessato, con particolare riferimento alla riservatezza b. acquisizione dei principi-concetti di semplificazione, armonizzazione ed efficacia nell'esercizio dei diritti e delle libertà da parte degli interessati, nonché nell'adempimento degli obblighi da parte dei titolari del trattamento; di necessità nel trattamento dei dati c. apprendimento dei contenuti tipici dell'Informativa come disciplinata dall'Art. 13 del Codice della privacy
Ulteriori regole per i trattamenti effettuati da soggetti pubblici	Il trattamento dei dati sensibili e giudiziari	a. conoscenza di presupposti, finalità e tecniche di trattamento di dati sensibili e giudiziari, con particolare riguardo per quelli contenuti in elenchi, registri o banche di dati tenuti con o senza l'ausilio di strumenti elettronici b. comprensione delle regole sul trattamento dei dati diversi da quelli sensibili e giudiziari
	Il trattamento dei dati personali da parte di privati ed enti pubblici economici	a. conoscenza delle condizioni di ammissibilità del trattamento b. apprendimento delle ipotesi di trattamento dei dati (anche sensibili), effettuato senza il consenso dell'interessato

Il trattamento dei dati personali in ambito sanitario	Principi generali, Informativa e Consenso	a. Cognizione dei principi cardine del trattamento dei dati personali, idonei a rivelare lo stato di salute, da parte degli esercenti le professioni sanitarie e degli organismi sanitari pubblici b. Conoscenza delle caratteristiche e dei contenuti dell'Informativa fornita dal medico di medicina generale o pediatra di libera all'interessato, nonché del Consenso da questi reso c. Individuazione concreta dei casi di raccolta dell'Informativa e del Consenso in forma semplificata da parte degli organismi sanitari pubblici e privati d. Conoscenza delle misure minime di sicurezza adottate in ambito sanitario e. Conoscenza delle cautele poste dall'Art. 84 del codice della privacy, in materia di accesso ai dati personali idonei a rivelare lo stato di salute da parte dell'interessato

Sicurezza informatica e Privacy dei dati nelle strutture sanitarie: riflessioni introduttive.	Aspetti tecnici e organizzativi legati alla sicurezza di un sistema informatico	a. Apprendimento del concetto di "Computer Security", attraverso la definizione di Privacy e Secrecy b. Acquisizione di consapevolezza circa gli aspetti tecnici e organizzativi legati alla sicurezza di un sistema informatico, con riferimento a: A) Definizione delle Politiche di Sicurezza in ambito informatica; B) Attuazione delle Politiche così definite; C) Verifica della corretta attuazione e della efficienza delle misure adottate (Audit di sicurezza) c. Acquisizione del concetto e delle proprietà di un Piano di Sicurezza o Piano di continuità operativa oppure Piano di disaster recovery
Misure minime di sicurezza dei dati e dei sistemi, a protezione dei dati personali trattati con strumenti elettronici	Misure minime di sicurezza e prevenzione	a. Conoscenza delle misure minime di sicurezza e prevenzione, contro i rischi di distruzione o perdita (anche accidentale) dei dati, di accesso o divulgazione non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta
	Gli strumenti di identificazione in rete	a. Approfondimento delle caratteristiche e delle funzioni di Carta di identità elettronica (CIE) e Carta Nazionale dei Servizi (CNS) b. Cenno agli strumenti alternativi predisposti dalle amministrazioni pubbliche

	Sicurezza e segretezza delle comunicazioni: crittografia, algoritmi di firma digitale e certificati digitali	a. Carrellata dei metodi e delle tecniche per la sicurezza dei messaggi, la verifica dell'integrità dei contenuti e l'autenticazione degli utenti-interlocutori b. Comprensione dell'arte crittografica, degli algoritmi di cifratura a chiave privata (o algoritmi simmetrici) o a chiave pubblica, degli gli algoritmi di firma digitale e/o dei certificati digitali
	Misure minime di sicurezza nel trattamento di dati personali senza l'ausilio di strumenti elettronici	a. Sapere che è necessario aggiornarsi periodicamente circa l'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative b. Sapere che è necessario aggiornarsi periodicamente per recepire l'eventuale adozione di procedure di custodia degli atti e documenti affidati agli incaricati, e/o di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
Referti on-line, Fascicolo sanitario elettronico (Fse) e Dossier sanitario: introduzione alle "Linee guida"	Normativa europea e nazionale di riferimento	a. Generica conoscenza del contesto normativo europeo di tutela dei dati sanitari b. Individuazione della ratio sottesa alla elaborazione delle Linee guida in tema di Referti on-line, Fascicolo sanitario elettronico e Dossier sanitario

Cautele e misure di sicurezza informatica nel servizio di refertazione on-line: dalle Linee guida dell'Autorità Garante per la protezione dei dati personali, all'intervento legislativo nazionale	a. Conoscenza delle caratteristiche del servizio di refertazione digitale e degli obblighi in materia di trattamento dei dati, da parte degli operatori sanitari b. Conoscenza e consapevolezza delle cautele e misure da adottare, a seconda delle modalità di fornitura del servizio di refertazione on-line c. Acquisizione della capacità di raffronto tra contenuti disciplinari delle Linee guida e previsioni normative del DPCM dell'8 agosto 2013, emanato con l'intento di attuare effettivamente l'applicazione e-Health in esame
Trattamento dei dati mediante FSE e Dossier Sanitario e misure di sicurezza informatica secondo le Linee guida del Garante per la Privacy e secondo il Legislatore italiano	a. Comprensione delle definizioni e dei contenuti del Fascicolo sanitario elettronico (FSE) e del Dossier sanitario b. Apprendimento delle modalità di esercizio del diritto del paziente alla costituzione di un Fse o di un dossier sanitario: requisiti e contenuti di informativa e consenso dell'interessato c. Individuazione dei soggetti abilitati al trattamento dei dati contenuti nel Fse/dossier d. Individuazione dei soggetti cui l'accesso e consultazione sono preclusi e. Conoscenza degli obblighi e delle facoltà del titolare del trattamento dei dati sanitari mediante Fse/Dossier sanitario

E-Health: Soluzioni ed applicazioni digitali in ambito sanitario

Malgrado le potenzialità dell' eHealth in termini di accrescimento della qualità dei servizi e delle prestazioni sanitarie, di maggior garanzia di continuità assistenziale, di efficiente utilizzo delle risorse finanziarie pubbliche, nelle aziende sanitarie spesso si è venuto a determinare uno scenario di resistenza all'innovazione a causa di diversi fattori, quali: la scarsa partecipazione, da parte delle direzioni sanitarie, a progetti caratterizzati da un alto rischio strategico ed una elevata complessità; l'incerto clima istituzionale e la ridotta capacità d'investimento legata alla scarsità di risorse a disposizione del servizio sanitario nazionale (SSN); la debole attitudine all'investimento in ricerca e sviluppo nel campo delle tecnologie mediche.

Con la lettura del presente Modulo didattico, si vuole contribuire:

- ad informare l'utenza dei benefici e delle utilità potenzialmente derivanti dall'uso di queste nuove tecnologie;
- a diffondere, tra professionisti sanitari e cittadini-pazienti, un clima di fiducia nei servizi di eHealth, favorendone l'accettazione;
- ad avere una discreta comprensione del contesto, normativo ed operativo, in cui collocare le varie applicazioni di eHealth.

Invero, le summenzionate applicazioni consentiranno di:

- supportare il monitoraggio dei livelli essenziali di assistenza sanitaria;
- migliorare l'efficienza delle cure primarie, attraverso l'integrazione in rete dei professionisti sanitari;
- supportare l'integrazione dei servizi sanitari e sociali nell'ambito del territorio, al fine di agevolare i processi di assistenza domiciliare, l'integrazione tra presidi, distretti e professionisti, e la continuità assistenziale;
- contribuire efficacemente al compimento degli interventi di prevenzione attiva;
- facilitare l'accesso ai servizi, potenziando e facilitando la scelta dei cittadini attraverso l'interoperabilità tra i sistemi;
- migliorare la qualità dei servizi sanitari e favorire il consolidamento e lo sviluppo delle eccellenze, attraverso l'introduzione di soluzioni orientate al governo clinico, alla formazione continua in medicina, e alla telemedicina;
- supportare il controllo della spesa sanitaria, attraverso il monitoraggio della domanda di prestazioni sanitarie

ARGOMENTO	AMBITI DI INTERVENTO	TESTING DI COMPETENZA
Introduzione	Benefici e vantaggi dell'innovazione tecnologica in ambito sanitario	a. Conoscenza degli principali novità introdotte dal d.l. 179/2012 in materia di sanità digitale
Il panorama normativo comunitario e nazionale della sanità elettronica	Raccomandazioni e Comunicazioni della Commissione europea, Piano di Sviluppo Nazionale 2003-2005, Piano Sanità elettronica, Piano industriale per l'innovazione della P.A., Linee guida sul Fascicolo sanitario elettronico, Patto per la sanità digitale 2014-2016	a. Conoscenza del processo di regolamentazione, a livello europeo e nazionale, della sanità elettronica
Carta d'identità elettronica, Tessera Sanitaria e Carta Nazionale dei Servizi: insieme verso il Documento digitale unificato	TS-CIE e TS-CNS	a. Conoscenza delle principali tappe del processo di unificazione della CNS con la TS, della CIE con la TS, nonché della creazione del documento digitale unificato
Il Centro unificato di prenotazione (CUP) ed il nuovo modello di farmacia dei servizi	CUP e Farmacia dei Servizi	a. Conoscenza dei vantaggi e delle comodità legate al nuovo modello di Farmacia dei Servizi
I Certificati di malattia on-line	Attori e compiti all'interno del processo di generazione e trasmissione del certificato di malattia on-line	a. Comprensione dell'ambito di applicazione e delle caratteristiche peculiari del processo di trasmissione telematica dei certificati di malattia all'Inps, con particolare riguardo ai soggetti coinvolti e agli strumenti tecnologici di supporto

La ricetta "dematerializzata" ai blocchi di partenza	Promemoria cartaceo della ricetta digitale	a. Conoscenza della nuova modalità di prescrizione medica, mediante ricetta dematerializzata, con attenzione alle caratteristiche e funzioni del Promemoria cartaceo della ricetta digitale, alle fasi del processo di trasmissione dei dati tra MMG/PLS - SAC - Struttura sanitaria
Il referto on-line	Posta elettronica del paziente, autenticazione informatica dell'utente e download del documento sanitario	a. Acquisizione di informazioni circa l'esistenza e funzionamento del servizio di consegna on-line del referto, attivato da molte strutture sanitarie.
La Cartella clinica elettronica	Forma, struttura e contenuti della CCE	a. Conoscere i contenuti, gli elementi strutturali e di sicurezza, e le modalità di utilizzo della Cartella clinica elettronica
Il fascicolo sanitario elettronico (FSE) e l'attuale scenario normativo	Linee guida sul FSE	a. Conoscere le Linee guida sul FSE del 16.07.2009, dell'11.11.2010, e del 31.03.2014
	Il processo di creazione del FSE: garanzie e adempimenti preliminari, contenuti strutturali e finalità sottese	a. Comprensione delle finalità connesse alla costituzione del FSE; dei contenuti e delle modalità di informativa ed acquisizione del consenso alla creazione del FSE; distinzione fra consenso generale al trattamento dei dati personali mediante FSE e consensi specifici sulle informazioni da rendere visibili o meno, sui soggetti del SSN da abilitare all'accesso ai dati ivi contenuti; consapevolezza delle forme di consultazione del FSE da parte del cittadino; individuazione del contenuto minimo di un FSE; conoscenza del valore legale dei dati raccolti nel FSE

	La gestione del FSE: ruoli, profili e modalità di accesso	a. Individuazione di compiti e responsabilità del Titolare e del Responsabile del trattamento dei dati personali, con riferimento anche alle ipotesi di cotitolarità b. Conoscenza delle modalità e degli strumenti di accesso al FSE da parte dei soggetti abilitati
	Caratteristiche principali di un'infrastruttura di sanità elettronica	a. Comprensione dei concetti di disponibilità delle informazioni, di sicurezza e privacy, di accesso e organizzazione modulare al FSE
Introduzione alla Telemedicina	La Telemedicina	a. Conoscere i riconoscimenti istituzionali, a livello internazionale e nazionale, dell'importanza della Telemedicina
	I servizi di Telemedicina: classificazione, finalità sanitarie e soggetti coinvolti	a. Conoscenza delle finalità sanitarie proprie dei servizi di telemedicina b. Acquisizione delle capacità di classificazione dei servizi; di individuazione e distinzione dei soggetti coinvolti nel processo di creazione di un atto sanitario di telemedicina
Web 2.0 e medicina: le nuove tecnologie di aggregazione, collaborazione e scambio, al servizio di medici e pazienti	Web 2.0 e salute	a. Conoscere le opportunità di aggregazione sociale e le inevitabili criticità legate al web 2.0 in ambito medico

info@eipass.com