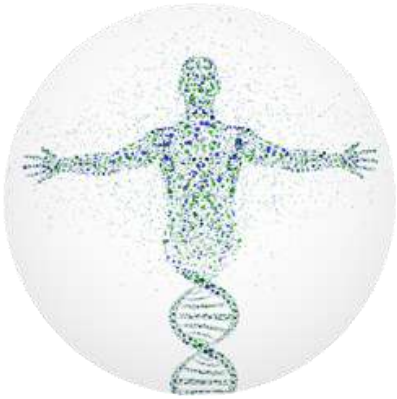
european informatics passport



EIPASS **Sanità Digitale**

Programma analitico d'esame

Premessa

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 (come vedremo) 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.

Sono questi i principali temi affrontati da questo programma di certificazione di competenze informatiche, dedicato specificamente al mondo della sanità e alla formazione dei relativi operatori, in quel processo di individuazione delle skills professionali e di susseguente realizzazione di percorsi ad hoc che Certipass promuove, per offrire progetti sempre più rispondenti alle esigenze degli attori principali di settori specifici della nostra società e del mondo del lavoro.

Certipass

Comitato Tecnico-Scientifico

Programma analitico d'esame EIPASS Sanità Digitale

Con il termine e-health, di recente conio, si fa riferimento al complesso delle risorse, soluzioni e tecnologie informatiche di rete applicate in ambito sanitario.

Il Percorso di certificazione EIPASS 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.

Si indicano di seguito gli argomenti oggetto di analisi e di verifica dei cinque moduli previsti:

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

Modalità di certificazione e valutazione

Il rilascio della certificazione avverrà previo sostenimento e superamento di esami online (1 per modulo). Ciascuna sessione avrà una durata di 30 minuti.

Nel corso della sessione il Candidato dovrà effettuare 30 test inerenti il modulo interessato, consistenti in domande a scelta multipla, quesiti vero/falso o simulazioni operative. I test saranno selezionati dal Sistema di rete in modalità casuale. Sarà sempre il sistema che calcolerà la percentuale di risposte esatte fornite decretando il superamento o meno dell'esame ed esprimendo in merito la valutazione dello stesso: non essendovi alcun intervento da parte di un Docente Esaminatore, viene garantita l'obiettività dell'esito conseguito.

L'Esaminatore, figura autorizzata da Certipass previo conseguimento di apposita qualifica, si limiterà quindi al controllo del rispetto delle previste procedure.

La valutazione finale sarà espressa in percentuale. Ciascun esame si riterrà superato previa l'attribuzione al Candidato di una percentuale minima di risposte esatte pari o superiore al 75% del totale. L'eventuale, mancato superamento di uno o più dei previsti moduli comporterà la ripetizione degli stessi attraverso una prova suppletiva.

1 Informatica di base ed internet

Obiettivo del modulo

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
1.0 Conoscere i concetti generali della Tecnologia dell'Informazione	1.0.1 Analisi di base componenti hardware	a. Indicare la corretta accezione di base del termine "hardware" b. Indicare i principali componenti hardware di un computer
	1.0.2 Classificazione dei computer	a. Descrivere un computer, definendo le differenze caratterizzanti le varie tipologie disponibili (PC, notebook, laptop, smartphone, mainframe, ecc.)
	1.0.3 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
	1.0.4 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.)
	1.0.5 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

1.1 Ottimizzare le risorse	1.1.1 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
1.2 Comprendere i concetti generali per la gestione di un sistema operativo ad interfaccia grafica	1.2.1 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 b. risoluzioni schermo, ecc.) c. Indicare la corretta procedura di installazione di un "software applicativo" d. Indicare la corretta procedura di disinstallazione di un "software applicativo"
1.3 Comprendere le modalità e le funzionalità di gestione di file e cartelle	1.3.1 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

	1.3.2 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
	1.3.3 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
1.4 Utilizzare un Browser per la navigazione in rete	1.4.1 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

1.4.2 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

1.5 Utilizzare efficacemente un motore di ricerca	1.5.1 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
1.6 Utilizzare servizi di posta elettronica	1.6.1 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

	1.6.2 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
1.7 Utilizzare aree riservate per la condivisione e la trasmissione di dati e documenti	1.7.1 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

2 Digitalizzazione e archiviazione documentale

Obiettivo del modulo

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
2.0 Digitalizzazione e archiviazione documentale	2.0.1 L'archivio e i flussi documentali	a. Concetto di archivio b. Classificazione c. Fascicolo d. Flussi documentali
	2.0.2 Gli "oggetti" dell'archivio digitale	a. Regole per l'archiviazione e conservazione dei documenti in formato digitale b. Documenti analogici obbligatori
2.1 Documenti informatici	2.1.1 La dematerializzazione degli archivi	a. Definizioni introdotte dal Codice dell'Amministrazione Digitale (CAD)
	2.1.2 La disciplina probatoria dei documenti informatici	a. Validità dei documenti informatici b. Apposizione di firma digitale
	2.1.3 Le copie	a. Art. 22 del CAD b. Copie di documenti informatici e loro validità c. Procedure di validazione
2.2 Conservazione dei documenti informatici	2.2.1 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
	2.2.2 Il Responsabile della conservazione	a. Funzioni b. Conformità del processo

	2.2.3 Il Manuale della conservazione	a. Elementi essenziali b. Fasi del processo di conservazione sostitutiva
	2.2.4 Nuove regole tecniche per i sistemi di conservazione	a. Regime transitorio
2.3 Firma elettronica	2.3.1 Evoluzione	a. Introduzione b. Primi certificatori accreditati c. Gli organi di vigilanza
	2.3.2 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
	2.3.3 Le firme elettroniche nell'Unione Europea	a. Direttive comunitarie b. Divergenze con la normativa nazionale c. Le Decisioni più recenti
	2.3.4 Legislazione nazionale	a. Tipologie definite dal CAD
	2.3.5 Firma elettronica	a. Firme elettroniche non verificabili b. SSCD c. Firma elettronica avanzata
	2.3.6 Firma digitale	a. Definizione b. Caratteristiche c. Firma elettronica qualificata

2.3.7 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
2.3.8 Base tecnologica	a. Crittografia b. Crittografia e firma digitale
2.3.9 Processo di generazione	a. Fasi della generazione di una firma digitale
2.3.10 Verifica della firma digitale	a. Fasi del processo di verifica

3 Protezione elettronica del dato personale

Obiettivo del modulo

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
3.0 Privacy: definizione ed evoluzione	3.0.1 Privacy come diritto alla riservatezza	a. Origini b. Carta dei diritti fondamentali dell'Unione europea
	3.0.2 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
3.1 Codice in materia di protezione dei dati personali	3.1.1 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
	3.1.2 Figure connesse alla protezione dei dati personali	a. Il garante b. Il titolare c. L'interessato d. Il responsabile e. L'incaricato
3.2 I diritti dell'interessato	3.2.2 Cosa può chiedere ed ottenere	a. Diritto a ottenere informazioni sul trattamento dei propri dati b. Diritto alla modifica e alla cancellazione dei propri dati.
3.3 Le regole in materia di protezione dei dati personali	3.3.1 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

	3.3.2 Criticità	a. Responsabilità civile b. Danni e risarcimenti c. Cessazione del trattamento
3.4 Le regole specifiche per i soggetti pubblici	3.4.1 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
	3.4.2 Dati sensibili	a. Normativa b. Autorizzazioni c. Raccomandazioni del Garante
	3.4.3 Banche dati	a. Visibilità e riservatezza b. Big data c. Open data
3.5 Privacy e diritto di accesso	3.5.1 Esigenze in conflitto: trasparenza e imparzialità contro riservatezza	a. Diritto di accesso b. Condizioni in cui il diritto alla privacy non risulta prioritario
3.6 Il consenso al trattamento dei dati personali	3.6.1 Consenso in forma scritta	a. Art.23 Codice della Privacy
	3.6.2 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
3.7 Le misure di sicurezza	3.7.1 Adozione misure per la protezione dati	a. Art.34 del Codice Privacy b. Art.35 del Codice Privacy c. Misure minime
	3.7.2 Aggiornamento periodico e controllo	a. Novità in materia di sicurezza nel Codice della Privacy b. Decreto semplificazioni c. Reato di frode informatica

	3.7.3 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
3.8 Il disaster recovery	3.8.1 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.

4 Sicurezza informatica e Privacy dei dati sanitari

Obiettivo del modulo

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
4.0 I principi generali	4.0.1 Sintesi dei principi e delle regole generali in materia di protezione dei dati personali	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
4.1 Ulteriori regole	4.1.1 Il trattamento effettuato da soggetti pubblici	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
	4.1.2 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

4.2 L'ambito sanitario	4.2.1 Il trattamento dei dati personali	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

4.3 Sicurezza informatica e Privacy dei dati nelle strutture sanitarie	4.3.1 Riflessioni introduttive	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
4.4 Misure minime di sicurezza dei dati e dei sistemi	4.4.1 Protezione dei dati personali trattati con strumenti elettronici	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
	4.4.2 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

	4.4.3 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
	4.4.4 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
4.5 Strumenti utilizzati in ambito sanitario. Linee guida	5.5.1 Referti on-line, Fascicolo sanitario elettronico (Fse) e Dossier sanitario	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

5.5.2 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
5.5.3 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

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

Obiettivo del modulo

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
5.1 Introduzione	5.1.1 L'innovazione tecnologica in ambito sanitario	a. Conoscenza degli principali novità introdotte dal d.l. 179/2012 in materia di sanità digitale b. Analisi dei benefici e vantaggi derivanti, per i cittadini ed il SSN, dall'innovazione tecnologica in ambito sanitario
5.2 Il panorama normativo comunitario e nazionale della sanità elettronica	5.2.1 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 elettronica, Patto per la sanità digitale 2014-2016	a. Conoscenza del processo di regolamentazione, a livello europeo e nazionale, della sanità elettronica
5.3 Il Centro unificato di prenotazione (CUP) ed il nuovo modello di farmacia dei servizi	5.3.1 Vantaggi del nuovo modello	a. Conoscenza dei vantaggi e delle comodità legate al nuovo modello di Farmacia dei Servizi
5.4 I Certificati di malattia on-line	5.4.1 La trasmissione telematica	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
5.5 La ricetta "dematerializzata" ai blocchi di partenza	5.5.1 La nuova prescrizione	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

5.6 Il referto on-line	5.6.1 Il nuovo servizio on-line	a. Acquisizione di informazioni circa il servizio di consegna on-line del referto, mediante posta elettronica del paziente, o con preventiva autenticazione informatica dell'utente e download del documento sanitario
5.7 La Cartella clinica elettronica	5.7.1 L'utilizzo efficiente	a. Conoscere i contenuti, gli elementi strutturali e di sicurezza, e le modalità di utilizzo della Cartella clinica elettronica
5.8 Il fascicolo sanitario elettronico (FSE) e l'attuale scenario normativo	5.8.1 La normativa di riferimento	a. Conoscere le Linee guida sul FSE del 16.07.2009, dell'11.11.2010, e del 31.03.2014
	5.8.2 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

	5.8.3	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
	5.8.4	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
5.9 Introduzione alla Telemedicina	5.9.1	I riconoscimenti istituzionali	a. Conoscere i riconoscimenti istituzionali, a livello internazionale e nazionale, dell'importanza della Telemedicina
	5.9.2	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
5.10 Web 2.0 e medicina: le nuove tecnologie di aggregazione, collaborazione e scambio, al servizio di medici e pazienti	5.10.1	Le opportunità ed i rischi del web 2.0	a. Conoscere le opportunità di aggregazione sociale e le inevitabili criticità legate al web 2.0 in ambito medico