

PNRR FSE 2.0 Incremento competenze digitali - **PROGRAMMA 11** identità digitale, strumenti digitali, dematerializzazione, cybersecurity

## Personale di studio medico MMG/PLS

### ORE FORMATIVE 15

<b>IDENTITA' DIGITALE - "INTER-WEB" (3h)</b>		
<b>Finalità</b>	<b>Contenuti</b>	<b>Durata (min)</b>
Approfondire la comprensione delle normative e delle best practice per la gestione sicura delle identità digitali nel contesto sanitario	Regolamento Generale sulla Protezione dei Dati (GDPR): approfondimento e analisi delle implicazioni specifiche generate nel settore sanitario	<b>40</b>
Fornire consapevolezza sulla importanza della privacy e della protezione dei dati personali nel contesto delle identità digitali	Normative e responsabilità: il ruolo del personale ASL nella protezione dei dati personali	<b>30</b>
Acquisire competenze pratiche per la gestione sicura delle identità digitali, includendo la creazione, l'autenticazione e la gestione degli account digitali	Principi di sicurezza informatica: Linee Guida per la creazione e la gestione sicura e protetta degli account digitali	<b>40</b>
Promuovere la consapevolezza sull'importanza della comunicazione e della collaborazione sicura in ambienti digitali, fornendo strumenti e linee guida per la condivisione protetta delle informazioni tra i colleghi e con i pazienti	Comunicazione sicura nell'assistenza sanitaria: strumenti e pratiche per la condivisione sicura e protetta delle Informazioni	<b>30</b>
Identificare le potenziali minacce informatiche che possono compromettere le identità digitali e fornire strategie per prevenirle e affrontarle efficacemente	Le minacce informatiche nel settore sanitario: rischi potenziali e strategie di difesa per la protezione e la tutela delle identità digitali	<b>40</b>

### DIFFUSIONE STRUMENTI DIGITALI - FUNDAMENTALS (3h)

<b>Finalità</b>	<b>Contenuti</b>	<b>Durata (min)</b>
Approfondire le tematiche afferenti alla normativa nazionale dei diritti/doveri di accesso ai dati personali; conoscere ruoli e responsabilità del personale sanitario per il rispetto della normativa vigente	Normativa Nazionale su diritti e doveri di accesso ai dati personali: contenuto normativo; diritti fondamentali dei cittadini in merito all'accesso ai propri dati personali e responsabilità delle organizzazioni nel rispettare tali diritti	<b>30</b>
Conoscere le funzionalità e le modalità di utilizzo dell'FSE, con particolare riguardo alla ricerca della documentazione e alla relativa consultazione; approfondire gli ulteriori servizi online esistenti	Aderenza alle Linee Guida di Attuazione del FSE	<b>30</b>
Conoscere un Sistema Informativo Sanitario (SIS) e comprendere l'importanza e l'utilità per la gestione delle informazioni e dei dati clinici e amministrativi dei pazienti	Sicurezza e Privacy dei Dati nel Contesto del SIS: normative e best practices che garantiscono la sicurezza e la privacy dei dati dei pazienti all'interno del Sistema Informativo Sanitario; formazione sulle misure di sicurezza fondamentali e sulle azioni per prevenire accessi non autorizzati o violazioni della privacy	<b>30</b>
Approfondire il ruolo del Sistema Informativo Sanitario nel processo di trasformazione dei dati in informazioni utili a supportare il processo decisionale; sfruttare i dati per l'efficientamento dei servizi e il miglioramento della qualità dell'assistenza offerta	Utilizzo efficace delle informazioni e delle conoscenze fornite dal Sistema Informativo Sanitario; pratiche migliori per integrare l'istruzione sull'uso del SIS nel processo formativo del personale sanitario, garantendo una corretta comprensione e applicazione delle informazioni	<b>30</b>
Comprendere la composizione dei documenti presenti all'interno del Sistema Informativo Sanitario (SIS); conoscere le principali informazioni contenute nei fascicoli sanitari dei pazienti	Il ruolo delle cartelle cliniche dei pazienti nel SIS: cartelle cliniche dei pazienti come componente essenziale di un Sistema Informativo Sanitario (stato di salute, storia clinica e trattamenti ricevuti da ciascun paziente); corretta compilazione, aggiornamento e conservazione delle cartelle cliniche	<b>30</b>
Approfondire le informazioni contenute nelle cartelle cliniche elettroniche (CCE) dei pazienti: dati anamnestici, diagnosi, piani di cura, esami diagnostici e procedure correlate	Struttura e Contenuto delle Cartelle Cliniche Elettroniche (CCE): struttura tipica delle cartelle cliniche elettroniche, inclusi i dati anamnestici, le diagnosi, i piani di cura e gli esami diagnostici; sezioni principali presenti nelle CCE e informazioni specifiche contenute in ciascuna sezione	<b>30</b>

**DEMATERIALIZZAZIONE - FUNDAMENTALS (3h)**

<b>Finalità</b>	<b>Contenuti</b>	<b>Durata (min)</b>
-----------------	------------------	-------------------------

<p>Conoscere la relazione e la differenza esistente fra archivi di popolazione, cartelle cliniche personali e fascicoli sanitari; analizzare gli impatti conseguenti alla transizione da cartaceo a digitale</p>	<p>Vantaggi e benefici della digitalizzazione dei dati sanitari per il personale sanitario e per i pazienti: riduzione degli errori di registrazione, facilità di condivisione delle informazioni tra operatori sanitari e migliore tracciabilità delle cure</p>	<b>30</b>
<p>Analizzare, in termini di costi e benefici, l'impatto della digitalizzazione dei Sistemi informativi Sanitari (SIS): disponibilità delle informazioni, miglioramento assistenza del paziente, efficientamento processo di cura</p>	<p>Analisi dei Costi e dei Benefici dell'Informatizzazione dei Sistemi Sanitari (SIS): costi associati all'implementazione e alla manutenzione dei SIS (investimenti in tecnologia, formazione del personale e infrastruttura informatica); benefici derivanti dall'informatizzazione (riduzione errori di registrazione e ottimizzazione delle risorse sanitarie)</p>	<b>30</b>
	<p>Impatto delle informazioni migliorate sul Processo di Cura: effetti positivi che le informazioni più affidabili e tempestive producono sul processo di cura (miglioramenti nella diagnosi, pianificazione del trattamento e monitoraggio della salute del paziente)</p>	<b>30</b>
<p>Formare sull'utilizzo della firma digitale, con particolare riguardo alle tematiche della sicurezza e dell'affidabilità dello strumento digitale</p>	<p>Introduzione all'importanza della firma digitale nel contesto medico e della conformità legale nelle pratiche mediche</p>	<b>30</b>
	<p>Sicurezza e affidabilità della firma digitale</p>	<b>30</b>

## SICUREZZA E PROTEZIONE INFORMATICA - "INTERMEDIATE" (6h)

Finalità	Contenuti	Durata (min)
<p>Conoscere le principali disposizioni nazionali relative alla legge sulla privacy e sulla protezione dei dati personali: GDPR e Linee Guida per l'utilizzo dell'FSE</p>	<p>Normative sulla privacy e la sicurezza dei dati, come il GDPR e le specifiche tecniche AICA</p>	<b>30</b>
	<p>Conformità normativa e aggiornamento delle Linee Guida del FSE</p>	<b>30</b>
<p>Conoscere le implicazioni della Normativa sulla Privacy nell'Utilizzo del SIS</p>	<p>Esplorazione delle sfide e delle opportunità nell'adattare i processi e le procedure dell'ASL alla normativa vigente sulla privacy e protezione dei dati personali</p>	<b>60</b>

Comprendere le peculiarità dei diversi metodi di autenticazione: password, card/tokern, scansione biometrica, strong authentication	<p>Approfondimento del concetto di Autenticazione Multifattoriale, che utilizza più metodi di verifica dell'identità per accedere ai dati sensibili o ai sistemi informativi; modalità attraverso cui l'autenticazione multifattoriale offre un livello aggiuntivo di sicurezza rispetto alla tradizionale autenticazione basata solo su password</p> <p>Metodi di Autenticazione Basati su ciò che un utente sa (es. password o PIN, che richiedono la conoscenza di informazioni segrete per confermare l'identità dell'utente); vantaggi e limitazioni di questo metodo di autenticazione e delle best practice per la creazione e la gestione di password sicure</p> <p>Metodi di Autenticazione Basati su ciò che un utente possiede (es. card o token, che richiedono il possesso fisico di un dispositivo o di una chiave per accedere ai sistemi); come questi metodi possano migliorare la sicurezza e i rischi associati alla perdita o al furto del dispositivo di autenticazione</p>	<b>30</b> <b>30</b> <b>30</b>
Approfondire le tematiche relative alla sicurezza degli strumenti informatici: analisi dei comportamenti virtuosi da agire e delle best practice da condividere all'interno dell'organizzazione	Importanza del cambio regolare delle Password per garantire la sicurezza dei dati e proteggere gli account dagli accessi non autorizzati; rischi associati al mantenimento delle stesse password per lunghi periodi e degli impatti negativi sulla sicurezza dei sistemi informativi;	<b>30</b>
Apprendere l'importanza di possedere password forti ed efficaci e di gestire in maniera strutturata e consapevole qualsiasi meccanismo di autenticazione	Il ruolo cruciale della password o di altri meccanismi di autenticazione: l'importanza di scegliere una password sicura o altri meccanismi di autenticazione robusti per proteggere l'accesso ai sistemi e ai dati sensibili	<b>30</b>
	Le caratteristiche della password o di altri meccanismi di autenticazione (es. lunghezza, complessità e varietà di caratteri); best practice per la creazione e la gestione di password sicure o altri metodi di autenticazione affidabili	<b>15</b>
	Best practices per la gestione delle password e degli altri meccanismi di autenticazione, inclusa la frequenza del cambio, la memorizzazione sicura e la condivisione responsabile; strategie per implementare e mantenere meccanismi di autenticazione efficaci e adatti alle esigenze di sicurezza dell'organizzazione	<b>15</b>
Formare sulla gestione e sulla tutela delle proprie credenziali di accesso, in particolare sensibilizzando alla custodia appropriata di token, password e/o altri metodi di autenticazione	Gestione riservata delle password e degli altri metodi di autenticazione per prevenire accessi non autorizzati ai sistemi e ai dati sensibili, implicazioni della divulgazione non autorizzata delle credenziali di accesso e dei potenziali rischi per la sicurezza delle informazioni	<b>15</b>

	<p>Divieto di condivisione delle password o dei Token; spiegazione rischi e conseguenze che possono derivare dalla pratica non autorizzata di condividere le credenziali di accesso; politiche e linee guida che vietano la condivisione delle password e dei token e promuovono l'individuazione e la prevenzione dell'abuso delle credenziali di accesso</p>	<b>15</b>
	<p>Best Practice per la custodia dei token e delle password, comprese le misure di sicurezza fisica e logica per proteggere le credenziali di accesso da accessi non autorizzati; educazione e formazione del personale sulla gestione delle credenziali di accesso</p>	<b>30</b>