Istruzioni agli Autorizzati al trattamento dei dati all'interno dell'organizzazione dell'Azienda Ospedaliera Ospedali Riuniti Marche Nord

PRINCIPI GENERALI

Al fine di una corretta applicazione dei principi e delle disposizioni contenute nel Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali, il soggetto autorizzato è tenuto – nell'ambito delle attività di trattamento effettuate presso la Struttura di appartenenza sotto la diretta autorità del designato in qualità di Responsabile "interno" del trattamento - ad osservare le seguenti istruzioni impartite dal Responsabile medesimo, ovvero:

☐ effettuare le operazioni di trattamento dei dati personali (ivi compresi i dati sensibili e giudiziari) strettamente necessarie allo svolgimento delle attività cui si è preposti nell'ambito della Struttura di assegnazione;

☐ trattare tutti i dati personali di cui si viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni secondo liceità e correttezza e, comunque, in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza;

☐ verificare che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;

☐ accedere unicamente alle banche dati presenti presso la Struttura in cui si presta la propria attività lavorativa;

☐ mantenere assoluto riserbo sui dati personali di cui si viene a conoscenza nell'esercizio delle proprie funzioni;

☐ evitare l'uso di strumenti informatici personali e del telefono cellulare per il trattamento di dati personali e sensibili acquisiti durante l'attività di servizio; ciò vale anche in caso di rilascio pareri e consulenze;

☐ utilizzare il PC, internet e la posta elettronica attenendosi alle indicazioni e prescrizioni fornite dalla UOC Servizio Informatico;

☐ attenersi alle disposizioni aziendali in tema di conservazione ed archiviazione dei dati e di accesso agli archivi locali e centralizzati di raccolta dei dati.

L'Autorizzato effettua le attività di trattamento dei dati nell'ambito della Struttura di appartenenza sotto la diretta autorità del designato in qualità di Responsabile "interno" del trattamento, fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti.

PER I TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave);

- I documenti contenenti dati personali prelevati ed estratti dagli archivi per lo svolgimento dell'attività quotidiana devono esservi riposti a fine giornata;

- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro. In caso di allontanamento - anche temporaneo - dal posto di lavoro, adottare le misure in atto a propria disposizione (secondo le istruzioni ricevute) per evitare l'accesso ai dati personali trattati o in trattamento, da parte di soggetti terzi, anche dipendenti, non autorizzati;

- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento);

- Qualora sia necessario eliminare documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere frammentati in maniera tale da non essere più ricomponibili;

- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati, i quali devono impedire l'accesso a persone prive di autorizzazione;

- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

PER I TRATTAMENTI EFFETTUATI CON L'AUSILIO DI STRUMENTI ELETTRONICI

- Il trattamento di dati personali con strumenti elettronici è consentito agli Autorizzati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Autorizzato associato a una parola chiave riservata conosciuta solamente dal medesimo;

- La password deve essere modificata dall'Incaricato almeno ogni 90 giorni solari;

- La password deve essere composta da almeno otto caratteri comprendenti lettere maiuscole e minuscole, numeri e caratteri speciali;

- Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera;

- Aver cura di non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;

- In presenza di ospiti occorre lasciare attendere questi ultimi in luoghi in cui non siano presenti informazioni riservate o dati personali;

- Non si deve lasciare incustodito e accessibile lo strumento elettronico (p.c.) durante una sessione di trattamento. In caso di allontanamento, anche temporaneo, dal posto di lavoro, occorre attivare adottare la procedura c.d. "salva schermo";

- Se nell'ambito dell'utilizzo del sistema informatico attraverso il quale viene effettuata attività di trattamento di dati si rileva una problematica tale da compromettere la sicurezza dei dati stessi, l'Autorizzato è tenuto a darne immediata comunicazione al designato in qualità di Responsabile "interno" del trattamento;

- Si deve accedere unicamente alle banche dati presenti presso l'Unità Organizzativa in cui si presta la propria attività lavorativa;

- Evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;

- È fatto assoluto divieto di comunicare o diffondere i dati personali provenienti da banche dati aziendali in assenza dell'autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;

- Accertarsi che sul proprio *personal computer* sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;

- Sottoporre a controllo mediante il programma antivirus installato sul proprio *personal computer* tutti i supporti di provenienza esterna prima di eseguire *file* in essi contenuti;

- Non è consentito l'uso e l'installazione di *software* non aziendali senza l'autorizzazione della competente UOC Servizio Informatico;

- Assicurarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; in caso di dubbio procedere alla cancellazione del messaggio senza aprire gli allegati;

- La connessione ad Internet deve essere utilizzata esclusivamente per lo svolgimento dei propri compiti istituzionali;

- Informare il designato in qualità di Responsabile "interno" del trattamento in caso di incidenti di sicurezza o di eventuali anomalie che coinvolgono i dati personali;

- Osservare tutte le misure tecniche, organizzative e di sicurezza adottate a livello aziendale, oltre le eventuali ulteriori istruzioni che verranno comunicate dal Titolare o dal designato in qualità di Responsabile "interno" del trattamento.