Istruzioni operative per gli Incaricati del trattamento dei dati personali

Introduzione

Il presente documento costituisce un manuale con istruzioni operative per il corretto utilizzo dei sistemi informatici e per l'accesso agli archivi cartacei presenti nell'Azienda Sanitaria nell'ambito delle attività di trattamento dei dati personali. Lo scopo è quello di ridurre e contenere i rischi di danneggiamento o dispersione dei dati trattati dall'Azienda Sanitaria, a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartecei da parte del personale addetto al trattamento.

I dati personali devono essere trattati:

- in osservanza dei criteri di riservatezza;
- in modo lecito e secondo correttezza;
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Istruzioni agli incaricati del trattamento dei dati personali

Ai sensi del Codice in materia di protezione dei dati personali (D.lgs. 196/03), avuto riguardo alle attività svolte nell'ambito della Struttura o Area di appartenenza, l'incaricato dovrà effettuare trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal "Responsabile del trattamento" (nel caso in cui non sia stato designato, le istruzioni verranno fornite dal titolare del trattamento).

Le istruzioni vengono suddivise in funzione della modalità del trattamento che può essere con e senza l'ausilio di strumenti elettronici.

Trattamenti senza l'ausilio di strumenti elettronici

1. 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).
2. I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono esservi riposti a fine giornata.
3. I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.
4. 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).
5. Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
6. 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.
7. 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.
8. Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare.

Trattamenti con strumenti elettronici

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati 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'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
2. Non comunicare a nessuno le proprie password.
3. Non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata.
4. Non scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere.
5. Non usare come password parole che possano essere facilmente riconducibili all’identità dell’utente.
6. La password assegnata all’incaricato è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
7. La password deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
8. 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.
9. In presenza di ospiti fare attendere questi ultimi in luoghi in cui non siano presenti informazioni riservate o dati personali.
10. Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

11. Non installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione del Responsabile del trattamento. Non modificare le configurazioni hardware e software senza l'autorizzazione del Responsabile del trattamento.
12. Se si rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati se ne dà immediata comunicazione al Responsabile del trattamento.
13. Accertarsi che sul proprio computer sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva.
14. Sottoporre a controllo con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire files in essi contenuti.
15. Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati.
16. Non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.
17. Utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali.
18. Non diffondere messaggi di posta elettronica di provenienza dubbia.
19. Non utilizzare servizi di comunicazione e condivisione di files.
20. Segnalare qualsiasi anomalia o stranezza di comportamento al Responsabile del trattamento.

Il Direttore Generale
Dott. Domenico Stalteri