REGOLE VINCOLANTI PER CIASCUN INCARICATO DEL TRATTAMENTO

All'atto della raccolta di dati personali è necessario verificare con la massima attenzione l'esattezza, la pertinenza, la completezza e la non eccedenza degli stessi rispetto ai fini perseguiti. Si invita ciascun incaricato a raccogliere e registrare i dati personali per scopi conformi alle finalità perseguite dall'ente. E' necessario aggiornare periodicamente i dati raccolti. I dati dovranno essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni dovranno essere trattati in modo lecito e secondo correttezza; non si dovranno portare fuori dal contesto dell'Ente supporti informatici o cartacei contenenti dati personali, salvo casi eccezionali che dovranno essere preventivamente autorizzati dal titolare o dal responsabile. Non comunicare o diffondere dati personali comuni a soggetti pubblici se non previsto da norma di legge o regolamento o risulti necessario per lo svolgimento delle funzioni istituzionali. In tale ultimo caso dovrà previamente comunicarlo al titolare o al responsabile del trattamento. Non comunicare o diffondere dati personali oggetto del trattamento privati o a enti pubblici economici se non previsto da norma di legge o regolamento. E' doveroso osservare scrupolosamente tutte le misure di sicurezza in atto o quelle che saranno successivamente adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti. I dati personali relativi allo stato di salute devono essere comunicati agli interessati solo tramite un medico designato dall'interessato o dal titolare. I dati devono essere cancellati o distrutti al termine degli obblighi legali di conservazione dei documenti. Evitare di comunicare per telefono informazioni relative a dati sensibili giudiziari. In caso di necessità identificare il chiamante e richiamarlo successivamente. Ciascun incaricato deve operare in modo tale da garantire che i dati afferenti lo stato di salute siano conservati in modo che non vi possano accedere persone prive di autorizzazione. In particolare gli archivi e i supporti ove sono allocate le cartelle cliniche devono essere costantemente presidiati. Ciascun incaricato è tenuto a conformarsi ad un comportamento coerente con le disposizioni in materia di riservatezza prescritte dal d.lgs 196/2003 e a prendere visione delle procedure individuate dall'Ente anche tramite la Guida Formativa disponibile presso gli Uffici Amministrativi. E' fatto dovere di conformarsi alle politiche di gestione e utilizzo degli strumenti elettronici elaborate dall'Ente ai sensi delle Linee Guida del Garante Privacy di data 01 marzo 2007.

REGOLE PER IL TRATTAMENTO CON STRUMENTI ELETTRONICI

L'accesso ai dati e/o agli strumenti elettronici è consentito agli incaricati unicamente con l'inserimento di un codice identificativo personale e di una password. La password è personale e segreta. Si invita quindi l'incaricato a non comunicarla a terzi. La password deve essere obbligatoriamente modificata dall'incaricato al primo utilizzo e successivamente ogni tre mesi in caso di trattamento di dati sensibili o giudiziari e ogni sei mesi per le altre tipologie di dati. La password scelta dovrà 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. La password non dovrà contenere riferimenti agevolmente riconducibili all'incaricato. Nel caso in cui l'accesso ai dati sia consentito tramite dispositivi di autenticazione (smart card), essi dovranno essere custoditi diligentemente dall'incaricato. Se l'Ente ha nominato il custode delle password, la password deve essere comunicata, ad ogni cambio, a tale persona la quale è autorizzata, in caso di assenza dell'incaricato, ad aprire la busta al fine di accesso ai dati per necessità di intervento tecnico, operativo o di sicurezza. Il custode delle password provvederà alla tempestiva informazione all'incaricato dell'intervento effettuato. Gli strumenti elettronici in dotazione degli incaricati non devono essere lasciati incustoditi o accessibili da terzi durante una sessione del trattamento. In caso di allontanamento dalla propria postazione di lavoro, il computer deve essere spento o bloccato (premere i tasti Ctrl + Alt + Canc – blocca computer) oppure deve essere attivata la procedura di screen saver con password o deve essere chiusa a chiave la porta di accesso agli uffici. Eventuali dati personali non coperti da salvataggio centralizzato (ad esempio quelli contenuti nel disco fisso del PC in dotazione) devono essere salvati dagli incaricati con frequenza almeno settimanale. I supporti utilizzati per il salvataggio dovranno essere custoditi a cura degli incaricati in cassetti, armadi, contenitori chiusi a chiave. Tutti i supporti rimovibili (come ad esempio floppy, cassette, CD), se non vengono più utilizzati devono essere distrutti o resi inutilizzabili. Tali supporti possono comunque essere riutilizzati, anche da altri incaricati, se le informazioni precedentemente in essi contenute non sono intelligibili o tecnicamente in alcun modo ricostruibili. Si raccomanda la totale formattazione dei supporti utilizzati. Se non fosse possibile formattare completamente i supporti utilizzati, gli stessi devono essere distrutti. Se i supporti rimovibili contengono dati sensibili o giudiziari devono essere custoditi a cura dell'incaricato al fine di evitare accessi non autorizzati o trattamenti non consentiti. Si consiglia quindi di conservarli in armadi o cassetti chiudibili a chiave.
I software e gli strumenti informatici devono essere utilizzati solamente per i fini strettamente necessari allo svolgimento del proprio lavoro. Gli accessi ad Internet e le caselle di posta non possono essere utilizzati per uso personale. Di regola non utilizzare fax o posta elettronica per l'invio di documenti in chiaro contenenti dati

sensibili e giudiziari. Se strettamente necessario procedere alla trasmissione in due tempi diversi, comunicando al richiedente, in un primo tempo, un codice identificativo e inviando successivamente il documento privo del nominativo dell'interessato. In ogni caso porre attenzione alla digitazione del numero telefonico. Qualora si dovessero riscontrare malfunzionamenti o non conformità, comunicare l'accaduto al più presto al titolare o al responsabile del trattamento.

REGOLE PER I TRATTAMENTI CON STRUMENTI NON ELETTRONICI (CARTACEO)

Tutti gli incaricati sono tenuti al controllo e alla custodia degli atti e dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento. A tal fine si invitano gli incaricati a portare fuori dai propri uffici atti o documenti solo se strettamente necessario. Si dovrà mantenere assoluto riserbo sui dati personali di cui si viene a conoscenza nell'esercizio delle proprie funzioni, avendo cura di rimuovere a fine lavoro i documenti dalla scrivania / piano di lavoro. Tutti i documenti contenenti dati personali comuni devono essere conservati negli appositi archivi/armadi. Nessun documento deve essere lasciato sul proprio tavolo o postazione di lavoro in modo che sia accessibile ad altre persone. Al termine delle operazioni affidate, gli atti e i documenti devono comunque essere riposti negli appositi armadi/archivi o restituiti al responsabile del servizio. Particolare attenzione deve essere posta agli atti e ai documenti che contengono dati sensibili o giudiziari. L'incaricato deve provvedere alla loro custodia facendo in modo che ad essi non accedano persone non autorizzate. Al tal fine gli incaricati dovranno conservare tali atti o documenti ad esempio in un cassetto della scrivania o in una cartella chiusa o con altro sistema equivalente in caso di ingresso nell'ufficio di persone estranee all'ufficio stesso. Tutti gli incaricati devono inoltre controllare i propri archivi/armadi affinché non sia possibile l'accesso agli stessi da parte di persone non autorizzate. A tal fine vengono assegnate apposite chiavi per la chiusura degli armadi. Gli archivi/armadi dovranno essere chiusi a chiave al termine dell'orario lavorativo. I documenti cartacei che non sono più utilizzati devono essere resi illeggibili prima di essere cestinati.

ISTRUZIONI PER GLI ADDETTI ALLA MANUTENZIONE/GESTIONE DEGLI STRUMENTI ELETTRONICI:

L'accesso è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di competenza: E' consentito eseguire le operazioni strettamente necessarie a tali scopi. Qualora fosse necessario eseguire stampe per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova. Qualora fosse strettamente necessario accedere a files contenenti dati già esistenti (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione. Qualora fosse strettamente necessario raccogliere e conservare presso il centro di assistenza i data base, tali dati dovranno essere custoditi in modo tale che non possano essere accessibili da soggetti non autorizzati. Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali. Qualora si dovessero riscontrare malfunzionamenti o non conformità, comunicare l'accaduto al più presto al titolare o al responsabile del trattamento. Nel casi in cui sia necessario accedere ai dati attraverso i PC in dotazione agli incaricati attenersi alle seguenti indicazioni: in presenza dell'incaricato far digitare la password dall'incaricato stesso evitando di venirne a conoscenza; in mancanza dell'incaricato rivolgersi al custode delle password il quale provvederà all'inserimento della password. Nei casi in cui sia necessario accedere ai dati attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici. L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione. E' vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai data base dell'Ente.

Ai sensi dell'articolo 30 del codice in materia di protezione dei dati personali (d.lgs 196/2003) le persone indicate sono state incaricate del trattamento dei dati personali secondo l'ambito definito e prefigurato tenuto conto delle peculiarità e delle necessità afferenti alla singola classe di appartenenza.

Ogni incaricato è stato invitato a prendere visione delle istruzioni allegate e delle regole definite nella guida formativa messa a disposizione.