Regione Piemonte
Azienda Sanitaria Locale n° 14 - V.C.O.
Sede Legale : Omegna, Via Mazzini n. 117

All. n. 11 Nomina Incaricato del Trattamento dei Dati

Prot. n. Al Sig._____

Oggetto: Nomina Incaricato del trattamento dei dati.

Su delega del Direttore Generale, Titolare del trattamento dei dati per conto dell'A.S.L. n. 14 V.C.O., ed in attuazione dell'art. 30 del D.Lgs 30/6/2003 n. 196, La informo che, in quanto dipendente della suddetta Azienda con la qualifica di _____ , chiamato a trattare dati personali e sensibili nell'ambito delle proprie competenze lavorative, Lei ricopre anche il ruolo di **Incaricato del Trattamento**. Pertanto, nell'espletamento delle funzioni riferite alla qualifica da Lei posseduta, potrà effettuare il trattamento dei dati personali e sensibili inerenti le mansioni di competenza.

Le ricordo inoltre che, nello svolgimento di tale funzione, dovrà attenersi alle istruzioni impartite dal Titolare e dal suo delegato, rispettando scrupolosamente la riservatezza degli interessati, ed attuando i trattamenti di competenza in modo lecito e corretto, in conformità a quanto indicato nel D.Lgs n. 196/2003.

In particolare, nella gestione dei dati, dovrà osservare le seguenti modalità:

Accesso a banche dati : Le banche dati e gli archivi cui può accedere per il trattamento dei dati personali sono le seguenti:

_____
_____
_____
_____

Creazione e diffusione di dati : Nessun dato può essere utilizzato, trasmesso o diffuso all'esterno se non previa autorizzazione del Titolare o del Responsabile del trattamento.

Misure di sicurezza : Ogni incaricato é tenuto ad osservare tutte le misure di protezione e di sicurezza dirette ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito. Tali misure di protezione e sicurezza sono sintetizzate nel Manuale aziendale per la sicurezza del trattamento dei dati personali (in particolare si richiama l'**art. 8 "Misure di sicurezza"**, il cui testo viene allegato alla presente comunicazione), nel Regolamento aziendale per l'utilizzo di sistemi di videocontrollo, e nel Documento Programmatico sulla Sicurezza dei dati, disponibili sul sito INTRANET dell'Azienda.

Distinti saluti

Il Responsabile del Trattamento dei dati

Data_____ _____

Data_____ Firma per ricevuta e per accettazione

_____

Stralcio Manuale aziendale per la sicurezza del trattamento dei dati personali

ART. 8
MISURE DI SICUREZZA

Trattamenti con strumenti elettronici

Sistema di autenticazione informatica

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;

2. ad ogni incaricato sono assegnate individualmente una o più credenziali per l'autenticazione. Esse devono essere modificate dall'incaricato al primo utilizzo e, successivamente, ogni 90 giorni;

3. le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (userid) associato a una parola chiave riservata (password); sono ad uso esclusivo dell'incaricato e quindi dovranno essere conosciute solamente dal medesimo. L'incaricato dovrà adottare le necessarie cautele e la diligente custodia delle parole chiave;

4. la password deve essere mnemonica, ma non banale cioè non deve contenere riferimenti agevolmente riconducibili all'incaricato (date di nascita, nomi propri, ecc.). Deve essere alfanumerica, contenere almeno due cifre numeriche, una lettera Maiuscola ed un carattere speciale (parentesi aperte o chiuse, *, %, $, &, #, !, ?, =, ^, +) ed avere una lunghezza minima di 8 (otto) caratteri; non deve essere diffusa; non deve essere scritta su biglietti attaccati al computer o in altri luoghi facilmente accessibili;

5. il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi;

6. le credenziali di autenticazione non utilizzate da almeno sei mesi saranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

7. le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;

8. è fatto obbligo uscire dall'applicazione qualora si lasci incustodito il terminale ed attivare la richiesta di autenticazione sullo screensaver onde evitare accessi non autorizzati;

9.le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione (la diffusione è il dare conoscenza dei dati trattati a persone indeterminate. Il tipico esempio è l'elenco telefonico).

Sistema di autorizzazione

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

1. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615 quinquies del codice penale, mediante l'attivazione di antivirus da aggiornare con cadenza almeno mensile.

2. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati, a cura dell'amministratore di sistema, almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

3. Il salvataggio dei dati con frequenza almeno settimanale. Le copie di salvataggio dati devono essere conservate in luogo diverso da quello dove risiedono i dati.

4. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (ad esempio formattando il supporto).

5. Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, deve essere garantito in tempi non superiori a sette giorni.

Misure di tutela e garanzia

Quando ci si avvale di soggetti esterni alla struttura per provvedere alla esecuzione di misure minime di sicurezza, occorre ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Trattamenti senza l'ausilio di strumenti elettronici

Nel caso di trattamenti di dati personali effettuato con strumenti diversi da quelli elettronici o comunque automatizzati è stato altresì stabilito di:

- conservare i dati e i documenti ad essi afferenti, in armadi o cassetti dotati di serratura o di altri sistemi di chiusura che ne consentano un accesso selezionato, evitando che gli stessi siano collocati in spazi liberamente accessibili al pubblico (ad es. corridoi, sale di attesa, sale riunioni ecc.);
- trattare i dati e le pratiche con diligenza e cautela tali da evitare indebite acquisizioni di notizie ed informazioni da parte di soggetti estranei o non autorizzati;
- trasmettere dati sensibili all'interno dell'Azienda direttamente a mani del destinatario, ovvero in buste o pacchi sigillati riportanti la dicitura "Riservato";
- comunicare dati sensibili a mezzo telefono o fax solo in situazioni di particolare urgenza e gravità, e comunque previa adozione di tutte le misure ritenute più efficaci per evitare la divulgazione a soggetti estranei e non identificati.
- gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli incaricati per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione;
- gli incaricati devono controllare l'accesso agli archivi contenenti dati sensibili o giudiziari. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;
- gli archivi e i registri cartacei devono essere custoditi in locali muniti di serratura ed il personale addetto provvede a far sì che in sua assenza i locali siano sempre chiusi a chiave;
- l'accesso e la permanenza nei locali degli archivi di persone non incaricate del trattamento deve avvenire sempre in presenza di uno degli incaricati al trattamento o del Responsabile;
- può altresì accedere ai locali, per esigenze strettamente di servizio, personale della segreteria della Direzione. In tal caso l'accesso deve essere segnalato appena possibile agli incaricati o al Responsabile del trattamento.

Tutti i Dirigenti di Servizio, Unità Operativa Amministrativa e Sanitaria dovranno attenersi, per quanto di propria competenza, alle suddette misure di sicurezza nel trattamento di dati personali in qualunque modo questi siano raccolti disponendone e verificandone l'osservanza anche da parte dei propri collaboratori.

Le misure previste dal presente articolo devono essere applicate **immediatamente.**

Per i casi di complessa attuazione, non oltre sei mesi dall'adozione del presente manuale previa presentazione di relazione al Direttore Generale che dettagli le azioni che dovranno effettuare.
Per quanto non espressamente disciplinato dal presente manuale, si rinvia al Documento programmatico sulla sicurezza per il trattamento dei dati, predisposto ed aggiornato annualmente dal Responsabile della S.C. Centro Elaborazione Dati/Sistema Informativo dell'Azienda.

Con apposita deliberazione del Direttore Generale é stato approvato il Regolamento aziendale sulla videosorveglianza, che disciplina il trattamento dei dati personali effettuato mediante l'utilizzo di impianti di videocontrollo (senza registrazione e conservazione delle immagini) nelle strutture dell'A.S.L. 14 V.C.O..
L'attività di videocontrollo realizza la finalità di garantire la sicurezza degli ambienti ospedalieri e persegue, inoltre, il fine istituzionale di monitorare in tempo reale, con controllo a distanza, la situazione fisico/sanitaria di specifiche e particolari tipologie di pazienti ricoverati presso le strutture ospedaliere.

Non rientra nella disciplina del presente atto l'utilizzo di apparecchiature strumentali per la rilevazione ed il monitoraggio dei parametri vitali dei pazienti.