Istruzioni per lo svolgimento delle operazioni di trattamento

Per responsabile interno/esterno e per incaricato interno/esterno

Premessa

Scopo del presente documento è illustrare le norme comportamentali, organizzative e tecniche cui i responsabili e gli incaricati devono attenersi nello svolgimento delle operazioni di trattamento di dati personali, al fine di ridurre e contenere i rischi di danneggiamento o dispersione, perdita dei dati trattati dall'Azienda, a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartacei da parte del personale addetto al trattamento.

Ai sensi del D.Lgs. n. 196/2003, art. 4, lettera a), costituisce "trattamento" qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in banche dati.

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.

Ai sensi dell'art. 4, comma 1, lett. h) del D.Lgs. n. 196/2003 gli "incaricati" al trattamento sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Quando per l'esecuzione delle prestazioni istituzionali, in nome e per conto dell'Azienda, si assume il ruolo di responsabile o incaricato del trattamento, occorre attenersi alle seguenti istruzioni e a quelle ulteriori che verranno eventualmente impartite.

Istruzioni per il trattamento dei dati

Ai sensi del Codice in materia di protezione dei dati personali (D.lgs. n. 196/03), i dati possono essere trattati esclusivamente per le finalità istituzionali, non essendo lecito alcun accesso a dati non giustificato dalla necessità di adempiere agli obblighi derivanti dalle mansioni attribuite nell'ambito del rapporto di lavoro e di collaborazione con l'Azienda.

Avuto riguardo alle attività svolte nell'ambito della Struttura di appartenenza, l'Incaricato dovrà effettuare trattamenti di dati personali attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà/dovrà essere fornita dal "Responsabile del trattamento" o dal Titolare.

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

1. Trattamenti senza l'ausilio di strumenti elettronici

1.1 Custodia

- 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 dagli archivi per l'attività quotidiana, devono esservi riposti tempestivamente a fine utilizzo e comunque a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.2 Comunicazione

- 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).
- la consegna dei documenti ai destinatari deve avvenire secondo opportune modalità di sicurezza, in particolare utilizzando buste chiuse, oppure effettuando la consegna personalmente, in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.
- E' sempre necessario accertarsi che il tipo di spedizione adottato consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri e quindi non manomessi o alterati.
- Si raccomanda di non parlare mai ad alta voce, trattando dati personali al telefono, in presenza di terzi non autorizzati.
- E' proibito trasportare all'esterno del posto di lavoro qualsiasi documentazione contenente dati personali e sensibili per fini diversi da quelli ricompresi nell'ambito dell'attività lavorativa, fermo restando gli obblighi di custodia di cui al paragrafo 1.1.

1.3 Distruzione

- Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi o, in assenza, devono essere stracciati in modo da non essere più ricomponibili.
- I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile devono essere distrutti.

2. Ulteriori norme in caso di dati particolari (relativi alla salute)

Nel caso di dati particolari (dati relativi alla salute, dati genetici, dati biometrici) occorre rispettare le seguenti ulteriori norme comportamentali:

2.1 Custodia

- Quando i documenti che contengono dati sensibili e/o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi documenti devono essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
- 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.
- L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono 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 sono preventivamente autorizzate.

2.2 Modalità di comunicazione ai pazienti e ai terzi legittimati

- E' vietato fornire dati e informazioni di carattere sanitario per telefono qualora non si abbia la certezza assoluta sull'identità del chiamante.

- Nel caso in cui giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia occorre verificare preliminarmente l'identità del soggetto richiedente. Prima di inviare via fax documenti contenenti dati sensibili assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati. Sulla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, che contenga dati personali, si deve apporre la seguente formula: "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Il destinatario della presente comunicazione deve distruggere immediatamente la documentazione ricevuta e in ogni caso potrà essere ritenuto responsabile dell'uso non autorizzato delle informazioni ivi contenute, erroneamente acquisite".
- In base all'articolo 84 del Codice la comunicazione di dati personali idonei a rivelare lo stato di salute all'interessato o a terzi legittimati (esercenti la potestà legale, prossimi congiunti o familiari) può essere fornita solo da un medico designato dall'interessato o dal titolare.
- Qualora singoli Responsabili intendano designare altro personale sanitario a fornire informazioni, tale trattamento dovrà essere evidenziato nella lettera di incarico e dovranno essere anche fornite specifiche istruzioni sulle modalità e cautele che dovranno da questi essere adottate nella comunicazione.
- Prima di dare informazioni a terzi legittimati occorre comunque verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione e accertarsi, per quanto ragionevole, dell'identità dei soggetti richiedenti (i terzi legittimati sono rappresentati, a titolo esemplificativo, da genitori, fratelli, figli, coniugi o conviventi, nonni e nipoti, e da chi dimostra di avere la potestà legale sull'Interessato).
- Tutti gli operatori sono tenuti ad evitare di discutere sulle condizioni cliniche dei pazienti in pubblico o con qualsiasi altra modalità (es. social network, videoconferenza, ecc..), con riferimenti che rendano direttamente o indirettamente identificabile la persona.
- È fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'URP.

2.3 Modalità di trattamento della documentazione sanitaria

- Il rilascio di copia di documentazione sanitaria (tra cui le cartelle cliniche) è disciplinato dall'articolo 92 del D.Lgs. n. 196/2003. Considerata la natura dei dati contenuti in detti documenti, si rinvia al Regolamento aziendale sulla cartella clinica.
- In caso di trasferimento interno dei pazienti ricoverati tra i diversi Presidi o reparti occorre utilizzare per la documentazione sanitaria buste o raccoglitori, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato.
- Qualsiasi documento relativo ad attività sanitarie (referti di esami di laboratorio, referti di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusa direttamente all'Interessato. Il ritiro della documentazione sanitaria è ammesso anche da parte di persona delegata per iscritto dall'Interessato.
- Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati devono essere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardanti lo stato di salute della persona interessata (es. giustificativo per datore di lavoro).
- I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regole di tutela del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente.

Trattamenti con l'ausilio di strumenti elettronici

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione formate da un codice per l'identificazione dell'incaricato (user-id) e da una parola chiave riservata (password) conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione (es. smart card o token USB) in possesso e uso esclusivo dell'incaricato, oppure in una caratteristica biometrica.

Gli incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Le user-id individuali e le password usate per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se incaricati del trattamento).
- Le password devono essere mantenute riservate e cambiate periodicamente come da specifiche istruzioni.
- I supporti elettronici contenenti dati personali devono essere conservati in luogo sicuro in maniera analoga ai documenti cartacei.
- Assicurarsi di non lasciare incustodite le stampe contenenti dati sensibili specie se la stampante è condivisa con più utenti e si trova a distanza dalla postazione informatica. Le copie non necessarie devono essere distrutte.
- Non lasciare visualizzati sullo schermo, in assenza del personale incaricato, dati personali e impostare se necessario una password salvaschermo.
- Evitate di discutere, anche con colleghi, di informazioni relative a dati personali, se non attinenti al lavoro da svolgere.
- Al termine del trattamento chiudere sempre i programmi secondo le appropriate misure di sicurezza.

In caso di applicazioni informatiche che prevedono, per ciascun incaricato o per classi omogenee di incaricati, profili diversi di autorizzazione, il sistema garantisce l'accesso ai soli dati necessari per effettuare le operazioni di trattamento, e l'incaricato non deve comunque accedere a dati per i quali non è autorizzato.