Azienda Sanitaria Regionale Molise

ASREM

Azienda Sanitaria Regionale del Molise

ISTRUZIONI AI RESPONSABILI E AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS. 196/2003 E S.M.I.

Documentazione di supporto a cura della Struttura Aziendale di Presidio Privacy

Premesse

Il Codice in materia di Protezione dei dati personali, cd. Legge sulla Privacy, è stato adottato con D.Lgs. 196/2003.

Considerando che la Privacy deve essere rispettata in modo sostanziale in quanto finalizzata al rispetto della dignità della persona attraverso la riservatezza dei dati personali, risulta evidente che attenersi adeguatamente alle prescrizioni di cui al D. Lgs. 196/2003 e s.m.i., impone un rilevante impegno organizzativo all'interno di ogni struttura aziendale.

Lo scopo delle presenti istruzioni è quello di fornire un supporto pratico / informativo ai Responsabili e agli Incaricati del Trattamento per ridurre al minimo i rischi di danneggiamento e di dispersione dei dati in ragione di un trattamento non corretto.

Si raccomanda di completare la lettura del presente documento con le disposizioni contenute nel D. Lgs. 196/03.

Istruzioni per i responsabili e gli incaricati del trattamento dei dati personali.

Nel premettere che il Responsabile del trattamento dei dati personali è il soggetto che, attenendosi alle istruzioni impartite dal titolare, lo coadiuva nell'attività di governo del trattamento dei dati sensibili, e che l'incaricato è il soggetto che, sempre in osservanza di quanto disposto dal Titolare o dal Responsabile, se designato, è il soggetto autorizzato a compiere tutte le operazioni di trattamento dei dati proprie delle mansioni svolte, in attuazione dell'art. 29 comma 5 e dell'art. 30 comma 1, del codice privacy, si riportano di seguito le istruzioni alle quali devono attenersi i responsabili e gli incaricati nell'effettuare i trattamenti dei dati:

1.1. - Istruzioni di carattere generale per tutti i responsabili e gli incaricati:

- **mantenere il segreto** sulle informazioni di cui si venga a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni del trattamento, evitando di comunicare le informazioni a terzi. Si ricorda che l'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché eventuali responsabilità, a seconda della gravità e del tipo di infrazione, di natura amministrativa, civile e penale;
- **assicurarsi e vigilare affinché venga sempre fornita l'informativa,** all'interessato o alla persona presso cui si raccolgono i dati, nel rispetto delle modalità e della modulistica adottata dall'Azienda;
- **richiedere il consenso** per il trattamento dei dati riguardanti lo stato di salute della persona cui ci si appresta a fornire la prestazione sanitaria per finalità di tutela della salute (ovvero prevenzione, diagnosi, cura e riabilitazione) o dell'incolumità fisica dell'interessato, quando questo non sia stato già prestato, salva l'ipotesi in cui il trattamento sia reso necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;
- **procedere alla raccolta dei dati personali** con la massima cura verificando l'esattezza degli stessi, nonché la pertinenza e la non eccedenza rispetto alle finalità da perseguire;
- **utilizzare** i dati solamente nei limiti del profilo di autorizzazione consentito e per gli scopi determinati, espliciti e legittimi;
- **comunicare** i dati personali non sensibili né giudiziari a terzi solamente se espressamente previsto da una legge o da un regolamento; se il richiedente è un altro soggetto pubblico la comunicazione è ammessa anche per finalità istituzionali, previa autorizzazione dell'Azienda;
- **ricordare** che le operazioni di trattamento (ivi compresa la comunicazione) dei dati sensibili e giudiziari possono essere effettuate solo se autorizzate da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili sugli stessi e le finalità di rilevante interesse pubblico perseguite o tra le operazioni assentite ai sensi del Regolamento sul Trattamento su Dati Sensibili e Giudiziari approvato dalla Regione Molise;
- **avvisare il Titolare di** ogni richiesta, provvedimento, accertamento, controllo da parte del Garante o dell'Autorità giudiziaria per fatti attinenti all'applicazione della normativa privacy;

- **non diffondere dati idonei a rivelare lo stato di salute** nel rispetto dell'espresso divieto previsto dall'art. 22, comma 8 del codice privacy. Per diffusione si intende "*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*". Sarà cura, quindi, dei soggetti che redigono gli atti oggetto di pubblicazione di far sì che si rispetti il divieto considerato.

1.2. - Istruzioni specifiche per i responsabili e gli incaricati delle strutture che erogano prestazioni sanitarie (prevenzione, diagnosi, cura e riabilitazione dello stato di salute)

Il Garante per la protezione dei dati personali in data 09 novembre 2005 ha adottato, con riferimento all'art. 83 del codice privacy, un importante provvedimento con il quale ha inteso richiamare l'attenzione dei soggetti che operano in ambito sanitario – e, quindi, anche le aziende sanitarie territoriali e le aziende ospedaliere – in ordine alla necessità di adeguare il funzionamento e l'organizzazione delle strutture operative, con espresso invito ad adottare tutte le misure ritenute necessarie ed opportune per garantire il rispetto della dignità e il massimo livello di tutela dei pazienti. In attuazione dell'art. 83 del codice privacy e dei suggerimenti del Garante, si riportano di seguito le specifiche istruzioni alle quali devono attenersi tutti i responsabili e gli incaricati delle strutture operative aziendali che erogano prestazioni sanitarie di prevenzione, diagnosi, cura e riabilitazione dello stato di salute:

- **Dignità dell'interessato**.

La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria con particolare riguardo a fasce deboli quali disabili, fisici e psichici, minori e anziani, nonché - per effetto di specifici obblighi di legge o di regolamento – sieropositivi o affetti da infezione da Hiv, interruzione di gravidanza e persone offese da atti di violenza sessuale. Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino la visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti. I Responsabili delle strutture dove, per finalità didattiche, alcune prestazioni sanitarie vengono erogate in presenza di studenti autorizzati, oltre ad informare preventivamente ogni singolo paziente di tale modalità, devono adottare specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.

- **Riservatezza nei colloqui e nelle prestazioni sanitarie**.

Durante lo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), devono essere adottate idonee cautele per evitare che le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le stesse cautele devono essere adottate in occasione della raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

- **Richiesta notizie su prestazioni di pronto soccorso.**

La notizia o la conferma di una prestazione di pronto soccorso, richieste anche per via telefonica, possono essere fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso. Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti

dall'interessato. Le informazioni che possono essere fornite riguardano solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso e non anche informazioni più dettagliate sullo stato di salute dell'interessato. L'interessato – se cosciente e capace – deve essere preventivamente informato (ad. es. in fase di accettazione) e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

- **Dislocazione dei pazienti nei reparti**.

Il paziente cosciente e capace deve essere, all'atto del ricovero, informato e posto in condizione di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Deve essere altresì rispettata l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota nemmeno ai terzi legittimati. Quando sia stato manifestato dall'interessato un consenso specifico e distinto al riguardo, possono comunque essere fornite informazioni sul suo stato di salute ai soggetti dallo stesso indicati.

- **Distanza di cortesia.**

Nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato, tutti i punti accettazione devono essere muniti di strumenti idonei a garantire la distanza di cortesia per gli utenti. Tali strumenti possono essere costituiti, a titolo meramente esemplificativo, da una riga gialla di segnalazione posta a terra e da un cartello che indichi il rispetto della distanza di cortesia, o qualunque altro sistema, che garantisca il medesimo risultato.

- **Ordine di precedenza e di chiamata.**

Nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es. in caso di analisi cliniche) devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa (ad es. attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. nel caso di paziente disabile) possono essere utilizzati altri accorgimenti adeguati ed equivalenti come ad esempio il contatto diretto con il paziente. Deve essere assolutamente evitata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento operatorio).

- **Correlazione fra paziente e reparto o struttura**.

Devono essere adottate specifiche procedure per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato. Tali cautele devono essere adottate anche per le eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura come ad esempio le certificazioni chieste per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale. Analoghe garanzie, infine, devono essere adottate nel caso di spedizione di plichi postali evitando che sugli stessi appaiano informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato come l'indicazione della tipologia del contenuto del plico o del reparto mittente.

- **Comunicazione di dati all'interessato riguardanti il suo stato di salute.**

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da un medico o da un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente stesso (ad es. un infermiere autorizzato dal suo responsabile

del trattamento dei dati). Nel caso specifico della comunicazione all'interessato degli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

1.3. - Istruzioni specifiche per tutti i responsabili e gli incaricati per il corretto uso e la sicurezza degli strumenti aziendali e la protezione dei dati personali.

L'ASREM nella sua qualità di datore di lavoro, essendo tenuta ad assicurare la funzionalità ed il corretto impiego degli strumenti informatici da parte dei propri dipendenti, ha approvato con Provvedimento del Direttore Generale n. 1627 del 24 dicembre 2009, il "Regolamento Aziendale per l'utilizzo delle postazioni di informatica individuale, di utilizzo della posta elettronica e della rete Internet aziendale", con il quale ha disciplinato le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti dando utili informazioni per comprendere le azioni che ciascun dipendente può metter in atto per contribuire a garantire la sicurezza informatica di tutta l'Azienda. Di seguito vengono fornite le istruzioni per il corretto uso e per la sicurezza degli strumenti aziendali e la protezione dei dati personali:

1 - Utilizzo del personal computer in dotazione

1) utilizzare il personal computer in dotazione, esclusivamente per ragioni di lavoro e per conto dell'Azienda;

2) utilizzare per il proprio lavoro, soltanto computer di proprietà dell'Azienda, salvo espressa autorizzazione ad utilizzare un computer privato rilasciata dall'Azienda;

3) assicurarsi che quando si sta lavorando al computer nessuno possa conoscere i dati che si stanno digitando o i file su cui si sta lavorando, ponendo attenzione a posizionare il monitor in modo da evitare che persone estranee possano visualizzare la schermata di lavoro;

4) disconnettere la sessione di lavoro ogni qual volta si abbandona, anche momentaneamente, la propria postazione;

5) in alternativa a quanto disposto al punto 4), utilizzare lo screen-saver protetto con password in modo da evitare che in caso di prolungata assenza i dati possano essere accessibili a soggetti estranei;

6) spegnere il computer in caso di assenza prolungata dal posto di lavoro. Un computer accesso è maggiormente attaccabile in quanto raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Lasciare un computer acceso aumenta il rischio che un'interruzione dell'energia elettrica possa causare un danno. Spegnere il personal computer alla fine della giornata lavorativa, con l' eccezione degli elaboratori che per la loro funzione specifica devono necessariamente essere in funzione 24 ore su 24;

7) non lasciare mai incustodito un notebook aziendale in ufficio o in viaggio;

8) durante le missioni di lavoro, portare il notebook come bagaglio a mano, evitando di trasportare in borsa i codici identificativi e le parole chiave di sicurezza, nonché i supporti di memorizzazione con le copie di back-up;

9) non è consentito al dipendente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo autorizzazione preventiva del personale tecnico autorizzato;

10) le informazioni archiviate informaticamente devono essere quelle esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa;

11) costituisce buona regola la pulizia periodica (ogni sei mesi) degli archivi, con eventuale archiviazione dei file obsoleti o inutili;

12) la tutela della gestione di dati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo; è comunque vietato l'uso di supporti rimovibili per la memorizzazione dei dati sensibili;

13) non è consentita l'installazione di programmi diversi da quelli autorizzati dal CED ASREM.

2 - Password

1) non è consentita l'attivazione delle password d'accensione (bios), senza preventiva autorizzazione da parte del personale tecnico autorizzato;

2) la password, assegnata a ciascun responsabile e incaricato, deve essere prontamente sostituita al primo utilizzo e deve essere modificata con cadenza almeno trimestrale;

3) 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; non deve contenere riferimenti agevolmente riconducibili al titolare della stessa e deve essere generata preferibilmente senza un significato compiuto;

4) nello scegliere la propria password, devono essere utilizzati anche caratteri speciali e lettere maiuscole e minuscole;

5) la password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;

6) il titolare della password è responsabile di ogni utilizzo indebito o non consentito della stessa;

7) fare attenzione a non essere "spiati" durante la digitazione di una password o qualunque codice di accesso;

8) non permettere l'uso della propria password da parte di soggetti terzi, per cui solamente in caso di necessità richiedere la finalità della richiesta (intervento di assistenza o di manutenzione) e accertarsi dell'identità del soggetto che richiede la comunicazione della vostra password.

3 – Dati

1) I dati devono essere trattati con liceità e correttezza;

2) il trattamento dei dati è ammesso solamente per uno scopo determinato, esplicito e legittimo;

3) i dati oggetto di trattamento devono essere pertinenti, non eccedenti e completi rispetto alle finalità perseguite;

4) nel caso di trattamento di dati sensibili o giudiziari devono essere trattati i dati indispensabili per gli scopi del proprio agire.

4 – Supporti di memorizzazione

1) Se possibile, salvare sempre le informazioni confidenziali sul server di rete e non sull'hard disk del personal computer in dotazione;

2) non salvare informazioni di natura sensibile su floppy-disk;

3) le pen drive in cui sono memorizzati i dati personali devono essere conservate e non cedute a terzi;

4) nel caso di utilizzo di pen drive, per la memorizzazione di dati, fare attenzione a disinserire le chiavi dalle porte USB seguendo la procedura di disconnessione sicura;

5) nel caso in cui le pen drive siano consegnate a terzi per trasferire dati, assicurarsi che sulla chiave di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare la chiave a terzi, che potrebbero copiare le informazioni personali memorizzate;

6) eliminare documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili;

7) accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

5 – Posta elettronica

1) Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'azienda (con indirizzo dell'ente) esclusivamente per necessità di lavoro;

2) la personalizzazione dell'indirizzo di posta elettronica non comporta la sua "privatezza", trattandosi comunque di strumenti di esclusiva proprietà aziendale dati in gestione al dipendente al solo fine dello svolgimento delle proprie mansioni lavorative;

3) non è consentito utilizzare l'indirizzo di posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni assegnate;

4) non è consentita la trasmissione a mezzo posta elettronica di dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati;

5) evitare di rispondere a messaggi promozionali o di spamming;

6) evitare di trasmettere per posta elettronica contenuti che possano essere considerati di tipo molesto/osceno, razzista, pedo-pornografico o illegale, nonché aventi natura ingiuriosa o diffamatoria;

7) evitare di registrare il proprio indirizzo di posta elettronica su siti web sospetti e/o mailing list non direttamente correlate all'attività istituzionale aziendale;

8) tutti i messaggi di posta elettronica relativi alle attività lavorative dovranno contenere un avvertimento ai destinatari di seguito specificato: "Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazioni al mittente."

6 - Internet

1) Per motivi di sicurezza (accesso indesiderato da postazioni esterne) non è consentito l'accesso e la navigazione Internet se non a mezzo della rete aziendale e per fini esclusivamente lavorativi; è vietato l'utilizzo di modem personali se non espressamente e formalmente autorizzati dalla A.S.Re.M. Internet deve essere utilizzato esclusivamente per ragioni di lavoro;

2) è consentito navigare in internet esclusivamente in siti attinenti lo svolgimento delle mansioni assegnate;

3) è vietato accedere a siti web contenenti materiale pedo-pornografico, materiale fraudolento-illegale, materiale blasfemo/molesto/osceno;

4) è, altresì, vietato tentare di violare o aggirare i sistemi di controllo o di protezione dell'uso di internet e della posta elettronica installati e utilizzati dall'Azienda, nel rispetto del diritto alla riservatezza dei dipendenti;

5) è, infine, vietato installare e/o utilizzare in modo fraudolento strumenti concepiti per compromettere la sicurezza dei sistemi (ad esempio strumenti di "password cracking", "network probing",…);

6) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo casi espressamente autorizzati dalla Direzione Aziendale;

7) non è consentito lo scarico di software gratuiti e shareware prelevati da siti internet, salvo il software espressamente autorizzato dalla Direzione Aziendale;

8) è consentita unicamente la registrazione a siti i cui contenuti siano legati all'attività lavorativa;

9) è consentita la partecipazione, unicamente per motivi professionali a Forum, bacheche elettroniche e le registrazioni in guestbook;

10) la partecipazione a forme di social networking in forma di chatline come, ad esempio, Facebook, GMAIL, America online, etc. è espressamente vietata in ogni sua forma;

11) non è consentito l'uso e navigazione su siti tipo Xrated, casinò virtuali, Webchat basate su Java, siti Warez e similari;

12) non è consentito scaricare/scambiare materiale coperto da diritto d'autore.

7 – Rete di comunicazione

1) E' vietato allacciare alla rete di comunicazione aziendale strumenti elettronici che non siano stati forniti dall'Azienda;

2) il computer in dotazione non deve possedere o disporre di altri collegamenti esterni diretti;

3) è vietato installare mezzi di comunicazione propri (come per esempio il modem analogico);

4) utilizzare esclusivamente le installazioni messe a disposizione dall'azienda ovvero quelle che siano oggetto di specifica autorizzazione;

5) ricorrere, eventualmente, a sistemi esterni solamente per finalità istituzionali e di lavoro e se è necessario registrarsi, comunque, non usare mai il proprio nome utente (user-id o username) e la propria password aziendale;

6) ricordarsi che l'azienda può monitorare il lavoro svolto e le connessioni, potendo verificare quali siti siano stati visitati e quali operazioni di trattamento sono svolte con i dati personali, di cui è titolare l'azienda;

7) non inviare informazioni confidenziali tramite internet o altre reti di comunicazione elettronica senza aver preso le dovute precauzioni e adottato le misure di sicurezza idonee a ridurre i rischi di accesso abusivo dei dati trasmessi.

8 – Protezione da virus informatici

1) accertarsi che sul computer sia sempre operativo il programma antivirus aggiornato e con la funzione di monitoraggio attiva;
2) sottoporre a controllo con il programma installato sul proprio p.c. tutti i supporti di provenienza esterna prima di eseguire file in esso contenuti;
3) 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;
4) non condividere con altri computer il proprio disco rigido o una cartella di file senza password di protezione in lettura/scrittura;
5) proteggere in scrittura i propri floppy disk contenenti programmi eseguibili e/o file di dati;
6) limitare la trasmissione tra computer in rete di file eseguibili e di sistema;
7) non scaricare da internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

9 – Backup dei dati

Gli incaricati che trattano i dati sui propri p.c., per i quali non sono previsti back-up centralizzati, devono provvedere al back-up cioè al salvataggio dei dati di interesse in copie di sicurezza da effettuarsi periodicamente su cd o altri supporti . I supporti di back-up devono essere custoditi in luogo sicuro e ad accesso controllato. In occasione di ogni back-up, occorre sempre accertarsi dell'esito positivo della procedura. Tutti i Responsabili verificano la puntuale osservanza di siffatta prescrizione.

10 – Utilizzo di telefono e fax

1) In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando;

2) verificare comunque che l'interessato abbia autorizzato la comunicazione dei propri dati a terzi;

3) in alcuni casi, specie per chiamate di natura istituzionale (da altre strutture ospedaliere, autorità giudiziaria, soggetti pubblici), si consiglia di farsi lasciare dal chiamante il proprio nominativo e il numero di telefono; si provvederà a ricontattare l'ente chiamante, chiedendo della persona che ha lasciato il proprio nominativo, previa verifica dell'indispensabilità dei dati richiesti rispetto alla finalità dell'utilizzo dichiarato e della previsione normativa o dell'autorizzazione dell'interessato alla comunicazione dei propri dati;

4) nel caso in cui si debba procedere alla comunicazione di dati sensibili tra unità diverse utilizzando il fax, è opportuno che lo strumento sia collocato in un'area protetta e presidiata e che i responsabili e gli incaricati prestino attenzione alle fasi di invio (verifica della corretta digitazione del numero del destinatario, inserimento di formula di riservatezza) e di ricevimento della documentazione contenente dati personali sensibili;

5) nel caso in cui si debbano comunicare ad un ente o soggetto esterni dati sensibili utilizzando il fax, in occasione del primo rapporto con l'ente, si deve richiedere, prima dell'invio della documentazione, di indicare il numero di un fax, localizzato in luogo protetto e non accessibile al pubblico, al quale inviare la documentazione;

6) il riscontro alla richiesta di cui al punto precedente, avrà come effetto l'autorizzazione all'azienda ad inviare esclusivamente al numero dichiarato la documentazione considerata. Ogni operatore incaricato del trattamento deve conservare copia della comunicazione di elezione del numero di fax, indicato per la ricezione di fax riservati.

11 – Utilizzo della stampante

1) La stampa di documentazione contenente dati personali e sensibili deve avvenire ad opera di incaricati autorizzati a trattare tali dati;

2) ritirare tempestivamente la documentazione dalla stampante utilizzata;

3) il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nell' esclusiva disponibilità dell'incaricato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti;

4) i fogli contenenti dati personali e sensibili non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da rendere non intelligibili a terzi – usando eventualmente un dispositivo distruggi documenti – dati personali ivi contenuti.

12 – Utilizzo della fotocopiatrice

1) La fotoriproduzione di documentazione cartacea, contenente dati personali e, in particolare, dati sensibili deve avvenire ad opera dell'incaricato autorizzato a trattare tali dati.

1.4. - Istruzioni per i responsabili e gli incaricati per il corretto trattamento dei dati su supporto cartaceo.

Di seguito si riportano le istruzioni che tutti i responsabili e gli incaricati sono tenuti a rispettare quando il trattamento dei dati avvenga attraverso supporti cartacei:

- quando le cartelle cliniche o altra documentazione contenente dati idonei a rivelare lo stato di salute devono essere trasferite da una struttura o da un ufficio presso altro luogo (esempio archivio di deposito) è necessario utilizzare cautele per la protezione della riservatezza al fine di impedire un accesso non autorizzato a tale documentazione. Si consiglia di inserire la documentazione in busta chiusa o in raccoglitori sigillati sui quali apporre la propria firma per garantirne l'integrità;
- i locali adibiti ad archivio all'interno di ciascuna struttura, in cui siano conservati documenti contenenti dati personali di natura sensibile, devono essere chiusi a chiave e le chiavi devono essere custodite da personale autorizzato (accesso selezionato);
- evitare di scrivere dati personali di natura sensibile su lavagne o altri supporti che possano essere visionati da persone non autorizzate;
- le cartelle e i fascicoli di lavoro devono essere tenuti sulla propria scrivania facendo attenzione che i dati eventualmente riportati sul frontespizio non siano visibili a persone non autorizzate (es. utenti del servizio);
- nel caso di assenza, anche momentanea, dalla propria stanza, non lasciare incustoditi fascicoli, cartelle e documenti cartacei contenenti dati di natura sensibile. Si consiglia di chiudere a chiave la propria stanza, qualora rimanga incustodita senza personale all'interno, ovvero di riporre la documentazione dentro un armadio chiuso a chiave.

Norma finale

Per tutto quanto non espressamente previsto dalle presenti istruzioni si rimanda alle disposizioni di cui al D. Lgs. 196/2003 e s.m.i. ed alla normativa vigente in materia di trattamento dei dati personali.

AZIENDA SANITARIA REGIONALE MOLISE
Sede Legale: Via U. Petrella,1 – Campobasso
U.O. Privacy
Tel. 0875.7159375 – Fax 0875.7159386
C.F./P.IVA 01546900703

INDICE