" GUIDA OPERATIVA PER IL CORRETTO TRATTAMENTO DEI DATI DA PARTE DEL PERSONALE AMMINISTRATIVO E SANITARIO"

(Applicazione del D.Lgs 196/03- Codice in materia di protezione dei dati personali)

PREMESSA

Il diritto alla privacy ed, in particolare, alla protezione dei dati personali costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

Con l'entrata in vigore del Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali", (anche noto come Testo Unico o Codice sulla privacy),vengono definiti la modalità di raccolta dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni. Il Codice in pratica definisce in maniera chiara ed inequivocabile i diritti degli Interessati, cioè di coloro a cui si riferiscono i dati. Va chiarito che lo spirito della legge non è di impedire il trattamento dei dati, ma di evitare che questo avvenga contro la volontà dell'avente diritto, ovvero secondo modalità pregiudizievoli.

Il diritto alla privacy è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità.
E' di tutta evidenza il rilievo che la tutela della privacy assume in ambito sanitario, dove, in aggiunta alla tipologia dei dati trattati - pressoché esclusivamente di natura sensibile-, gli interessati si ritrovano, per lo più, in una condizione di fragilità, connessa ai problemi di salute.
Questa particolare condizione deve essere tenuta in debito conto da parte di tutti gli operatori coinvolti nel percorso assistenziale, per adeguare il loro agire a un'efficace tutela del diritto in oggetto.
Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori della sanità, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'Utenza.

Tuttavia,al rispetto della privacy si può pervenire non solo attuando gli adempimenti formali previsti dalla normativa, ma anche e soprattutto attraverso un graduale e continuo percorso informativo/formativo dei propri dipendenti e collaboratori, finalizzato a far maturare e crescere la cultura della privacy, condivisa dagli operatori sul campo.

Partendo da tale considerazione la Casa di Cura Montevergine ha ritenuto opportuno predisporre questo strumento contenente oltre che alcuni indispensabili elementi introduttivi sul Codice, anche le necessarie ed opportune istruzioni di carattere generale e specifico alle quali tutti i dipendenti e collaboratori – siano essi designati Responsabili o Incaricati - nell'ambito delle competenze formalmente assegnate, devono quotidianamente e scrupolosamente attenersi nello svolgimento delle operazioni di trattamento di dati Personali e Sensibili nei confronti dei pazienti/utenti, la cui Titolarità è della Casa di Cura Privata "Montevergine"S.p.A. e che devono essere ispirati alle direttive stabilite dal decreto legislativo 196/2003 (***Codice Privacy***), in particolare nel Titolo V della parte II intitolato *"Trattamento dei dati in ambito sanitario".*

Pertanto, la finalità della presente Guida , cui dovrà essere data ampia pubblicità, è quella di disciplinare le modalità di trattamento dei dati personali effettuati dalle unità operative della

Casa di Cura "Montevergine" affinché ciascun operatore possa svolgere la propria attività in modo tale da garantire quanto già esposto e cioè che il trattamento dei dati si effettui nel pieno rispetto dei diritti e delle libertà fondamentali, nonchè della dignità della persona.

E' opportuno evidenziare che nessuna guida operativa, per quanto dettagliata, potrà mai sostituire le intuizioni dettate dal buon senso e dal rispetto della dignità umana, valori certamente permeanti la personalità di tutti coloro che hanno scelto di lavorare in ambito sanitario e che la tutela della riservatezza dei dati del cittadino/utente non deve essere vissuta come un mero obbligo burocratico ma come strumento per offrire una reale tutela della riservatezza degli interessati, per i loro familiari e per tutti gli operatori attraverso un sistema che impegni ogni figura professionale presente in Azienda.

Se gli operatori aziendali hanno dubbi su come trattare in modo riservato i dati oggetto della loro attivita', l'Ufficio Privacy ha la funzione di chiarire le loro perplessita' e di indirizzare il loro lavoro per assicurare il rispetto della dignita' della persona in uno dei momenti di maggiore fragilita', cioe' quando si trova ad essere ammalato.

Il Titolare

Casa di Cura Privata "Montevergine" S.p.A.

DEFINIZIONI

Si ritiene utile riportare, per favorire una migliore comprensione del manuale, le principali definizioni di ordine generale previste dal DLgs 196/2003.

TRATTAMENTO.

Con il termine trattamento ci si riferisce ad una qualunque operazione effettuata sui dati svolta con o senza l'ausilio di mezzi automatizzati e che abbia come oggetto una delle operazioni indicate dall'art. 4, comma 1, lett. a) della Legge. 1) : raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione di dati, anche se non registrati in una banca di dati. Il trattamento comprende **l'intera vita** del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine. Di conseguenza, si parla di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano (documenti cartacei).

TIPOLOGIE DI DATI.

• **Dato Personale:** rappresenta qualunque informazione relativa a persona fisica che permette di identificarla in modo diretto (es. carta d'identita') o indiretto (ci si riferisce pure alle immagini, e ai dati biometrici come le impronte digitali). Quando una persona non è identificabile, i dati sono dichiarati anonimi

• **Dato Sensibile:** è il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i **dati personali idonei a rilevare lo stato di salute** e la vita sessuale dell'interessato. L'espressione "dati sanitari" si riferisce a tutti i dati a carattere personale relativi alla salute di una persona. Si riferisce egualmente ai dati aventi un collegamento stretto e manifesto con la salute così come i dati genetici.

L'elenco è tassativamente formulato dal Codice e non può essere ampliato anche di fronte al carattere di riservatezza o di particolare rilevanza che un soggetto, o il senso comune, può attribuire ad altre tipologie di dati (es. reddito).

• **Dato Giudiziario**: è il dato personale idoneo a rivelare i provvedimenti giudiziari penali ed amministrativi in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato (es.: provvedimenti di condanna definitivi, di proscioglimento, di non luogo a procedere per difetto di imputabilità, concernenti le pene, le misure di sicurezza, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere, le pene accessorie, le misure alternative alla detenzione, la liberazione condizionale, ecc.).

La distinzione tra le varie tipologie di dati personali assume notevole rilevanza in quanto i trattamenti vengono disciplinati in maniera differenziata in ragione della diversa natura del dato personale oggetto di trattamento riflettendosi anche sulle misure di sicurezza che dovranno essere adottate e previste dalla Legge. Il trattamento dei dati sensibili e, ancor più, dei dati sanitari e giudiziari, è sottoposto ad una tutela particolarmente rigorosa che comporta l'adozione di specifiche misure di sicurezza.

MODALITA' DI TRATTAMENTO DEI 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.
Relativamente al mezzo,essi possono essere trattati
1. **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. **con strumenti elettronici** (PC ed elaboratori).

TRATTAMENTI DEI DATI SANITARI.
La Casa di Cura Montevergine , come tutti gli organismi sanitari, pubblici e privati, può trattare i dati personali idonei a rivelare lo stato di salute per finalità di tutela della salute o dell'incolumità fisica dell'interessato **con il consenso dell'interessato e sulla base dell'autorizzazione a carattere generale del Garante**.
I due requisiti indicati possono essere richiesti alternativamente nelle seguenti ipotesi:
a) se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato è possibile procedere con il solo consenso dello stesso, anche senza l'autorizzazione del Garante;
b) se la finalità di tutela della salute o dell'incolumità fisica riguarda un terzo o la collettività è possibile procedere sulla base dell'autorizzazione del Garante, anche senza il consenso dell'interessato.
L'autorizzazione è soggetta a rinnovo periodico e rende superflua la richiesta di singoli provvedimenti autorizzatori da parte dell'Azienda.
I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

INFORMATIVA.
Il codice in materia di protezione dei dati personali, all'art.13, impone a coloro che trattano dati personali di terzi di rendere a questi ultimi un'esauriente informativa, oralmente o per iscritto.
La Casa di Cura Montevergine ha, pertanto, predisposto appositi moduli d'informativa, per i soggetti fisici e le persone giuridiche, i cui dati vengono trattati nell'esercizio della propria attività.
I moduli d'informativa contengono tutte le indicazioni richieste dalla normativa, ovvero: i motivi del conferimento dei dati, le modalità di loro raccolta, i requisiti degli stessi, le finalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale rifiuto di conferirli, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi, i diritti degli interessati, la ragione sociale, la sede del titolare cui rivolgersi per l'esercizio dei diritti riconosciuti dall'art.7, il riferimento al/i responsabile/i, individuato/i per funzione/i.
Per i primi trattamenti (ordinari), si è proceduto a formulare un'informativa "generale per il trattamento complessivo", destinata a pazienti/utenti che entrano in contatto con le strutture della Casa di Cura.
L'informativa fa riferimento a più trattamenti, siano essi finalizzati alla tutela della salute e dell'incolumità (per attività di prevenzione, diagnosi, cura e riabilitazione) od alla gestione amministrativa; ed è portata a conoscenza dei pazienti tramite consegna **al momento del contatto**

con la Casa di Cura , a mezzo affissione in tutti i luoghi accessibili all'utenza e pubblicata sul sito web aziendale.

Per i trattamenti più delicati, che presentano, cioè, rischi specifici (interventi chirurgici, procedure invasive) è prevista un'informativa specifica.

CONSENSO

Per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale è obbligatorio il consenso. Il consenso è qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di trattamento.

Il consenso ai sensi della normativa sulla privacy non deve essere confuso con il "consenso informato" necessario per poter sottoporre un paziente ad un determinato trattamento sanitario. In quest'ultima ipotesi, infatti, il paziente viene informato sul percorso diagnostico-terapeutico che gli viene proposto per poter decidere se sottoporsi a determinati accertamenti diagnostici, o trattamenti terapeutici, farmacologici o chirurgici.

Il consenso per il trattamento dei dati sanitari è acquisito in forma scritta sul modulo contenente l'informativa, che viene presentato al paziente e da lui sottoscritto prima dell'erogazione della prestazione sanitaria.

L'acquisizione del consenso al trattamento dei dati per le finalità di cura, **con l'eccezione delle prestazioni d'urgenza**, da parte dell'Azienda costituisce momento indispensabile e, pertanto, ha carattere d'obbligatorietà. L'eventuale rifiuto da parte dell'interessato di conferire il consenso al trattamento dei dati personali e sensibili, comporterà l'impossibilità da parte dell'Azienda di trattare i dati per le finalità indicate nell'informativa.

Il consenso, di norma, è preventivo.

L'informativa, ai sensi dell'art. 82 del Codice, ed il consenso al trattamento dei dati personali possono altresì essere dati, senza ritardo, successivamente alla prestazione (consenso tardivo), in caso di:

- emergenza sanitaria o igiene pubblica per la quale è stata emanata un'ordinanza da parte del Sindaco o altra pubblica Autorità (ad es. un'epidemia);
- impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'Interessato (per la gravità delle condizioni di salute ad es. il soggetto è trasportato d'urgenza in ospedale oppure è in stato di shock, oppure è demente o in stato di incapacità, anche temporanea, di comprendere il significato dell'informativa), quando non è possibile acquisire il consenso dai soggetti abilitati, da chi esercita legalmente la potestà (per le informazioni relative ai nascituri il consenso è prestato dalla gestante), ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'Interessato;
- rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'Interessato;
- in caso di prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia (es. il soggetto deve essere sottoposto ad una prestazione urgente ed indifferibile).

Il consenso deve essere acquisito ad ogni singolo ricovero; tale consenso, è considerato valido per la pluralità delle prestazioni erogate, da distinti Reparti ed Unità Operative di questa Casa di Cura , per trattamenti clinici e strumentali, a valenza sia diagnostica che terapeutica, necessari per la cura; tale consenso può essere in ogni momento rettificato o revocato da parte dell'Interessato; **il modulo diventa parte integrante di tutta la documentazione che costituisce la cartella clinica**.

Per i ricoveri d'urgenza (dei pazienti che passano per il Pronto Soccorso), gli adempimenti privacy

(in particolare l'acquisizione del consenso scritto) sono di competenza dei reparti.

SOGGETTI CHE EFFETTUANO IL TRATTAMENTO DEI DATI PERSONALI: TITOLARE, RESPONSABILI E INCARICATI.

Il trattamento dei dati personali è caratterizzato dalla presenza, dal lato attivo, del titolare del trattamento e, dal lato passivo, dell'interessato.

Dal lato attivo la nostra normativa contempla tre diverse figure, che possono coesistere nell'ambito di un processo di trattamento: **il titolare**, **il responsabile** e **l'incaricato** del trattamento.

Il **Titolare** del trattamento, ai sensi dell'art. 4 comma 1 lett. f), è "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza per la privacy".

Nel caso di specie Titolare del trattamento è la Casa di Cura Privata "Montevergine" S.p.A. come entità nel suo complesso nella figura del suo Rappresentante Legale.

Al Titolare competono dunque le decisioni in ordine alla modalità e finalità del trattamento dei dati personali ed alle misure organizzative utilizzate, in materia di privacy, ivi compreso il profilo della sicurezza per la privacy, nonchè il compito di vigilare, tramite verifiche periodiche, sull'osservanza delle disposizioni di legge, del regolamento e delle istruzioni impartite in materia di trattamento e di sicurezza per la privacy.

Nelle organizzazioni complesse, come può essere quella di un'azienda sanitaria, vi è la facoltà, da parte del Titolare, di provvedere alla designazione di uno o più **Responsabili del trattamento** che, come dispone l'art. 29 del codice devono essere individuati "*tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza".*

I Responsabili del trattamento dei dati garantiscono il rispetto della normativa sulla Privacy ed assicurano l'applicazione delle misure minime di sicurezza aziendali nonchè, alla luce delle indicazioni organizzative e procedurali fornite dal Titolare, sovrintendono alle operazioni di trattamento svolte dagli incaricati che operano presso la struttura da essi diretta

L'art. 30 del codice privacy prevede, inoltre, che "*le operazioni di trattamento possono essere effettuate solo da **incaricati** che operano sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni impartite*".

Vi è, di conseguenza, l'obbligo di procedere alla designazione, sempre per iscritto, in qualità di incaricati, di tutte le persone fisiche che a vario titolo sono preposte allo svolgimento delle operazioni di trattamento per conto del titolare – cioè dell'azienda – nonché impartire loro adeguate istruzioni.

Queste previsioni di carattere organizzativo sono state applicate nella Casa di Cura Montevergine designando, ognuno per le proprie funzioni e per le banche date e gli archivi gestiti negli ambiti di rispettiva competenza,

- quali **responsabili dei trattamenti,** tutti i Responsabili di Reparto, i Responsabili dei Servizi e degli Uffici e i soggetti esterni all'Azienda, per qualsivoglia forma di "outsourcing" che comportano un trattamento di dati personali/sensibili.
- quali **incaricati dei trattamenti,** tutto il personale dipendente e non (amministrativo e sanitario) e tutte le persone fisiche che a vario titolo svolgono temporaneamente attività all' interno della struttura (specializzandi, frequentatori, tirocinanti, collaboratori, stagisti).

La nomina degli incaricati, per i dipendenti a tempo indeterminato, è di durata pari a quella del rapporto di lavoro e decade per revoca, per dimissioni, o con il venire meno dei compiti che giustificavano il trattamento dei dati personali.
Per i collaboratori, i tirocinanti, gli stagisti, coloro che sono autorizzati a frequenze volontarie o a ricerche e/o tesi di laurea, master, ecc., la nomina quali incaricati è legata alla durata del loro rapporto con la Casa di Cura .
Ogni trattamento di dati personali consiste in un rapporto che si instaura tra Titolare ed Interessato.

- L'**Interessato** al trattamento, ai sensi dell'articolo 4, comma 1 lettera i), è "la persona fisica, a cui si riferiscono i dati personali" (Lettera così modificata dall'art. 40, comma 2, lett. b), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214

E' da considerarsi soggetto Interessato il paziente, l'utente, il consulente, il dipendente, il fornitore, il professionista, e quant'altri i cui dati sono raccolti e conservati nelle banche dati della Casa di Cura . L'Interessato può far valere personalmente o mediante delega, i diritti di cui all'art. 7 e ss. del D. Leg.vo n. 196/03,novellato.

NORME COMPORTAMENTALI PER RESPONSABILI ED INCARICATI

La **difesa della riservatezza** non è circoscritta ai dati contenuti in documenti; ma va **estesa a una pluralità di aspetti correlati all'erogazione di prestazioni sanitarie**.
In attuazione dell'art. 29 comma 5 e dell'art. 30 comma 1, del Codice, si riportano di seguito le istruzioni di **carattere generale** alle quali devono attenersi i Responsabili e gli Incaricati nell'effettuare i trattamenti dei dati:

- **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. **Segreto professionale**: tutto il personale del ruolo sanitario, tecnico, professionale e amministrativo, sia del comparto che della dirigenza, e chiunque presti la propria attività lavorativa, anche in veste di consulente, libero professionista o volontario, nei servizi o strutture dell'Azienda è tenuto al segreto professionale ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza delle notizie, dei dati o banche di dati di cui, in ragione e in occasione del proprio stato o ufficio, sia venuto a conoscenza.

Si ricorda che l'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dal Codice;

- **fornire l'informativa** all'Interessato o alla persona presso cui si raccolgono i dati, utilizzando la modulistica predisposta dall'Azienda e allegata al presente manuale;
- **raccogliere il consenso dell'Interessato** al trattamento dei dati idonei a rivelare lo stato di salute, ogniqualvolta si erogano prestazioni finalizzate alla tutela della salute (prevenzione, diagnosi, cura e riabilitazione), con le modalità e la modulistica definite dall'Azienda;
- **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 definito dal Responsabile del trattamento e per gli scopi determinati, espressi e legittimi;
- **comunicare i dati personali** di natura comune a terzi, solamente se espressamente previsto dalla legge;
- **comunicare i dati sensibili** solo a soggetti determinati e preventivamente e nominativamente individuati dall'Interessato (con le modalità e la modulistica definite dall'Azienda) o solo ove sia espressamente previsto dalla legge;
- **non diffondere dati idonei a rivelare lo stato di salute** nel rispetto dell'espresso divieto previsto dall'art. 22, comma 8 del Codice. 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. A titolo meramente esemplificativo, si suggerisce la necessità di predisporre la copia degli atti deliberativi da pubblicare, in una forma in cui vi sia il testo della stessa corredato da allegati (questi ultimi, contenenti i dati sanitari, non dovranno essere oggetto di pubblicazione, ma dovranno rimanere agli atti, conservati secondo quanto previsto dalla legge, e a disposizione di coloro che abbiano la legittimazione all'esercizio del diritto di accesso, secondo quanto previsto dalla legge 241/90, novellata)
- **prima di consegnare il referto medico verificare l'identità dell'interessato** sulla base di idonei elementi di valutazione (ad es. mediante l'esibizione di un documento di riconoscimento); nel caso in cui l'interessato abbia delegato un soggetto terzo al ritiro del referto, devono essere adottate analoghe cautele al fine di verificare l'identità del soggetto delegato consegnando il referto a quest'ultimo in busta chiusa.

Istruzioni <u>specifiche</u> 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, un importante provvedimento con il quale ha inteso richiamare l'attenzione dei soggetti che operano in ambito sanitario – e, quindi, anche 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 del suddetto art. 83 del Codice 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:

- **Tutela della dignità dell'Interessato**

La tutela della dignità personale deve essere sempre 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 – a pazienti sieropositivi o affetti da infezione da Hiv, a pazienti sottoposti a trattamenti medici invasivi o per i quali è doverosa una particolare attenzione (es. interruzione di gravidanza e persone offese da atti di violenza sessuale).

Nelle UU.OO. 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 le visibilità dell'Interessato, durante l'orario di visita, ai soli familiari e conoscenti.

- **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 (es. locali per più prestazioni) o dalle modalità utilizzate.

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

La notizia o la conferma di una prestazione, della presenza o del passaggio di una persona al pronto soccorso, richieste anche per via telefonica, possono essere fornite correttamente ai soli terzi legittimati e nominativamente indicati dall'Interessato, 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 (utilizzando la modulistica predisposta dall'Azienda per comunicazione dello stato di salute). Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

- **Dislocazione dei pazienti nelle UU.OO.**

Possono essere fornite informazioni sulla presenza dei degenti nelle UU.OO. ai soli terzi legittimati e nominativamente indicati dall'Interessato. 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 della U.O. di degenza (utilizzando la modulistica predisposta dall'Azienda);
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 nominativamente 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 sia per operazioni amministrative allo sportello (prenotazioni), sia al momento dell'acquisizione di informazioni sullo stato di salute, sensibilizzando anche gli utenti con cartelli, segnali ed inviti. 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) i pazienti non devono essere chiamati per nome, ma devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli Interessati, che prescinda dalla loro individuazione nominativa, 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.

- **Liste di pazienti**

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. Non devono essere resi visibili ad estranei documenti sulle condizioni cliniche dell'Interessato, come le cartelle infermieristiche poste vicino al letto di degenza o liste di pazienti in attesa di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento chirurgico).

- **Correlazione fra paziente e U.O. 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 della U.O. 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 della U.O. 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 di un altro esercente le professioni sanitarie che, nello svolgimento dei propri

compiti, intrattenga rapporti diretti con il paziente stesso (ad es. un infermiere autorizzato quale responsabile del trattamento dei dati).
Si possono dare informazioni sullo stato di salute a soggetti diversi dall'Interessato quando questi abbia manifestato uno specifico consenso (utilizzare la modulistica predisposta dall'Azienda per comunicazione dello stato di salute). In caso di impossibilità fisica o incapacità dell'Interessato o, valutato il caso, tale consenso può essere dato da un familiare o da persone legittimate a farlo (da chi esercita legalmente la potestà (per le informazioni relative ai nascituri il consenso è prestato dalla gestante), ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'Interessato).
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.

- **Ritiro delle analisi**

I referti diagnostici, i risultati delle analisi e i certificati rilasciati dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirati anche da persone diverse dai diretti Interessati purchè munite di delega scritta e con consegna in busta chiusa.

Istruzioni specifiche per il corretto uso e la sicurezza per la privacy degli strumenti aziendali e la protezione dei dati personali.

- **Utilizzo del personal computer in dotazione**

Il trattamento di dati personali (e ancor più di dati sensibili e giudiziari) attraverso l'uso di personal computer o video terminali richiede le seguenti misure di sicurezza per la privacy:
1) il trattamento di dati personali con personal computer è consentito soltanto ai Responsabili ed agli Incaricati dotati di password di accesso personale che consente il superamento di una procedura di autenticazione che consiste in un codice per l'identificazione associato ad una parola chiave riservata (password) conosciuta solamente del Responsabile o Incaricato;
2) utilizzare il personal computer in dotazione, esclusivamente per ragioni di lavoro e per conto dell'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) durante una sessione personale di trattamento e/o di lavoro il personal computer non deve essere lasciato incustodito ed accessibile ai non Incaricati;
5) in ogni caso di allontanamento, anche temporaneo, dalla postazione di lavoro, per sicurezza per la privacy, disconnettere la sessione di lavoro bloccando l'operatività del computer (es. logout, CTRL+ALT+CANC), da riattivare solo attraverso l'inserimento del Codice di accesso/password personali;
6) in alternativa al punto 5) 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;
7) 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;
8) quando vengono lanciate stampe di documenti, l'Incaricato del trattamento deve presidiare l'operazione e prelevare immediatamente i documenti stampati onde evitare la consultazione degli stessi da parte di persone non autorizzate;
9) è vietato modificare in alcun modo la postazione di lavoro (es. installazione di modem o schede

di rete o quant'altro) senza formale autorizzazione ed il presidio di un tecnico dell'ufficio informatico aziendale;
10) è vietato modificare le impostazioni di sicurezza per la privacy del PC (es. SW antivirus, impostazioni del browser, ecc.) senza formale autorizzazione ed il presidio di un tecnico dell'ufficio informatico aziendale;
11) non lasciare mai incustodito un notebook aziendale in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici);
12) 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 per la privacy, nonché i supporti di memorizzazione con le copie di back-up;
13) non lasciare esposto in automobile in sosta il notebook aziendale.
Il Responsabile della sicurezza informatica qualora rilevi, nell'esercizio della sua funzione, l'utilizzo improprio da parte del dipendente del personal computer in dotazione, relativamente ai punti da 2 a 10 sopracitati, dovrà predisporre apposita relazione in merito e proporre al Responsabile ., ove presta servizio il predetto dipendente, che nei confronti del predetto dipendente venga attivata il consequenziale provvedimento disciplinare; il Responsabile in questione dovrà attivare tempestivamente il suindicato provvedimento.

- **Username e Password**

1) L'Amministratore di sistema assegna a ciascun Responsabile o Incaricato autorizzato ad operare su una postazione di lavoro uno username come chiave di accesso riconducibile ad una singola persona. Le chiavi di accesso possono coincidere per lo stesso utente su diversi sistemi.
2) L'utente a cui viene assegnato per la prima volta uno username, riceve anche una password temporanea che dovrà modificare alla prima connessione. La password è il codice che rende "personale" la chiave, garantendone la riservatezza. La robustezza e segretezza delle password sono meccanismi fondamentali per la protezione di buona parte dei sistemi. Pertanto, la scelta della propria password deve rispondere ai seguenti **requisiti minimi**:
a) **Lunghezza**: dovrà avere una lunghezza minima di 8 caratteri alfanumerici (lettere e numeri) ed almeno due caratteri speciali e lettere maiuscole e minuscole;
b) **Complessità**: non deve contenere riferimenti agevolmente riconducibili al proprietario della stessa (es. data di nascita, nome dei figli, nome utente, etc.) e deve essere generata preferibilmente senza un significato compiuto;
c) **Ripetitività**: non potrà essere riutilizzata. Alla scadenza dovrà sempre essere impostata una password diversa da quelle impostate precedentemente;
d) **Scadenza**: la password assegnata deve essere prontamente sostituita al primo utilizzo e deve essere modificata con cadenza trimestrale;
3) la password deve essere comunicata per iscritto, in busta chiusa, dopo averne controfirmato i lembi, al Csustode delle Password che, potrà aprire la busta ed utilizzare la password (previa apposita verbalizzazione) nei casi di necessità previsti in assenza dal servizio dell'Incaricato;
4) all'atto della consegna della busta ciascun Incaricato dovrà firmare un apposito verbale di consegna datato;
5) le password non utilizzate da almeno sei mesi verranno disattivate;
6) le password sono disattivate anche in caso di perdita della qualità che consente al Responsabile o all'Incaricato l'accesso (es. trasferimento, pensionamento, etc.);
7) il proprio codice di accesso/password deve essere custodito con la massima attenzione e segretezza e non deve essere divulgato o comunicato a terzi o lasciarne una trascrizione in luoghi accessibili a terzi;
8) il possessore della password è responsabile di ogni utilizzo indebito o non consentito della stessa;

9) fare attenzione a non essere "osservati" durante la digitazione di una password o qualunque codice di accesso;
10) non permettere l'uso della propria password a soggetti terzi, per cui solamente in caso di necessità (intervento di assistenza o di manutenzione) richiedere la finalità della richiesta ed accertarsi dell'identità del soggetto che richiede la comunicazione della vostra password.

- **Supporti di memorizzazione**

1) se possibile, archiviare sempre i dati e tutti i documenti elettronici (word, excel, access…) utilizzati per effettuare trattamenti di dati personali sul server centrale di rete ed eliminarli dall'hard disk del personal computer in dotazione Questa misura di sicurezza per la privacy permette di proteggere con maggiore efficacia l'accesso ai dati da persone non autorizzate al trattamento
2) non salvare informazioni di natura sensibile su floppy-disk;
3) i supporti rimovibili (es. CD, DVD, pen drive, ecc.) contenenti dati personali devono essere conservati in strutture chiuse a chiave e mai lasciati incustoditi;
4) Se non più utilizzati, i supporti rimovibili contenenti dati sensibili o giudiziari devono essere distrutti;
5) 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;
6) i supporti rimovibili non vanno mai ceduti a terzi; nel caso in cui sono consegnate a terzi per trasferire dati, assicurarsi che sui supporti di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare i supporti stessi a terzi, che potrebbero copiare le informazioni personali memorizzate;
7) eliminare documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili utilizzando gli idonei distruggi documenti e distruggi CD;
8) accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

- **Virus**

1) i virus possono alterare o addirittura distruggere i dati e i programmi;
2) i virus diffusi in internet sono spesso camuffati da programmi di utilità o di intrattenimento;
3) ogni computer è protetto da idonei strumenti per il rischio di attività di virus informatici;
4) lo strumento di protezione (di norma software antivirus) è abilitato;
5) è vietato disattivare, senza autorizzazione, il software antivirus;
6) la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente;
7) nel caso di utilizzo di supporti di memorizzazione esterni, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto;
8) controllare periodicamente la presenza di virus sul personal computer in dotazione mediante la scansione dell'intero sistema.

- **Software**

L'impossibilità di applicare le misure di sicurezza per la privacy informatiche operate centralmente richiede l'applicazione delle seguenti misure di sicurezza per la privacy:
1) sul computer in dotazione può essere utilizzato solamente il software fornito dall'azienda;
2) non si possono installare software e applicazioni sul personal computer in dotazione senza una specifica autorizzazione da parte dell'Azienda ed il presidio di un tecnico del servizio informatico aziendale;

3) non creare e non utilizzare software senza licenza d'uso, È consentito unicamente l'utilizzo di software ufficialmente acquisiti ed inventariati dall'azienda.
4) provvedere al salvataggio (backup) degli archivi e documenti elettronici esistenti localmente sul personal computer con frequenza almeno settimanale;
5) adottare, relativamente all'accesso ai locali ove sono conservati i dati ed effettuati i trattamenti, misure di sicurezza per la privacy analoghe a quelle descritte per i trattamenti effettuati su supporto cartaceo (es. impedire l'accesso ai personal computer chiudendo a chiave le stanze).

- **Divieto di valutazioni automatizzate**

E' vietato adottare un atto amministrativo contenente una valutazione del comportamento umano fondandolo unicamente su un trattamento automatizzato di dati personali, volto a definire il profilo o la personalità dell'Interessato.
Pertanto in tutti i casi in cui l'Azienda si avvale di procedure informatizzate per monitorare, ad esempio, la presenza in servizio (timbrature), l'adozione di provvedimenti deve essere assunta valutando anche le altre circostanze.

- **Posta elettronica**

1) Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'azienda esclusivamente per necessità di lavoro;
2) i messaggi di posta elettronica ricevuti o spediti con l'indirizzo di posta elettronica aziendale non costituiscono corrispondenza personale del dipendente o collaboratore aziendali, per cui possono essere conosciuti da terzi per esigenze operative e istituzionali;
3) le informazioni trasmesse – molto spesso - possono/devono essere condivise per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti;
4) si deve evitare di rispondere ai c.d. "invii a catena" degli utenti di internet o ai messaggi di solidarietà che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici ovvero sistemi per la raccolta di indirizzi di posta elettronica, per l'invio di comunicazioni commerciali non desiderate o di posta cd. spazzatura;
5) evitare di rispondere a messaggi promozionali o di spamming;
6) evitare di trasmettere per posta elettronica contenuti che possano essere considerati di contenuto 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;

- **Internet**

1) Internet deve essere utilizzato esclusivamente per ragioni di lavoro;
2) non si deve utilizzare l'accesso ad internet per fini personali, che esulano dall'attività lavorativa;
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 per la privacy dei sistemi (ad esempio strumenti di "password cracking", "network probing",…).

- **Rete di comunicazione**

1) è 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 modem);
4) utilizzare esclusivamente le installazioni messe a disposizione dall'azienda ovvero quelle che siano oggetto di specifica autorizzazione;
5) non usare mai il proprio user-id e la propria password per accedere a sistemi esterni;
6) ricorrere, eventualmente, a sistemi esterni solamente per finalità istituzionali e di lavoro;

- **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'dentità 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 ed 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.
Il **fax** appare utile a garantire efficienza, economicità e velocità di comunicazione, tuttavia, presenta rischi specifici riguardo all'identità (a volte sconosciuta) di colui che materialmente riceve il documento trasmesso.
A tal proposito, prima di inviare documenti contenenti dati sensibili o per i quali vi siano particolari esigenze di riservatezza, è doveroso assicurarsi preventivamente che l'effettivo destinatario sia sul posto per riceverlo o che comunque non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati.
Sarebbe una corretta modalità di invio anticipare telefonicamente la trasmissione avendo cura di inserire in calce alla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, la seguente formula: *"Qualora il destinatario del presente fax non sia la persona indicata, è pregato di dare immediata comunicazione al mittente a mezzo telefono o fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta con l'avvertimento che in caso di non ottemperanza al presente invito si potrebbe essere ritenuti responsabili della mancanza di protezione e/o dell'uso non autorizzato delle informazioni erroneamente acquisite*
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;
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.

- **Utilizzo della stampante**

1) la stampa di documentazione contenente dati personali e sensibili deve avvenire ad opere 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 nella elusiva 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.

- **Utilizzo della fotocopiatrice**

La fotoriproduzione di documentazione cartacea, contenente dati personali e, in particolare, dati sensibili deve avvenire ad opera dell'Incaricato autorizzato al trattamento dati.

- **Utilizzo dello scanner**

coloro che provvedono all'acquisizione in formato digitale della documentazione cartacea devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati.

- **Spedizione di documenti contenenti dati personali a mezzo posta**

la documentazione contenente dati sensibili o giudiziari deve essere trasferita, anche all'interno dellA struttura, in busta chiusa, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti. Per dare garanzia della non apertura della busta e della integrità del contenuto sarebbe opportuno che i lembi della busta fossero sigillati e firmati. In alternativa è comunque opportuno piegare il documento spillandone i lati.

Istruzioni specifiche per gli incaricati addetti alla manutenzione e alla gestione degli strumenti elettronici e delle attrezzature elettromedicali.

Gli Incaricati addetti alla manutenzione e alla gestione degli strumenti elettronici e delle attrezzature elettromedicali, individuati ai sensi del punto 15 del Disciplinare tecnico allegato B al Codice, devono attenersi alle seguenti specifiche istruzioni:

- **verificare** in via preliminare e prima di iniziare la propria attività, l'esistenza e la disponibilità di copie di salvataggio dei dati memorizzati sugli strumenti elettronici oggetto di interventi di manutenzione;
- **verificare** la leggibilità dei dati memorizzati sui supporti contenenti le copie di salvataggio, informando gli utenti dei servizi della possibilità che alcuni dati potrebbero andare persi;
- **accedere** ai soli dati e informazioni indispensabili all'esecuzione delle azioni di assistenza e manutenzione;
- **tutelare** la riservatezza degli Interessati, mantenendo il segreto su ogni notizia e informazione, acquisite in occasione dell'attività di gestione e manutenzione degli strumenti elettronici;
- **richiedere** all'operatore la parola chiave di accesso ad una applicazione solo in caso di necessità, invitando lo stesso alla modifica della sua parola chiave terminato l'intervento tecnico di assistenza;
- **custodire** i supporti rimovibili di memorizzazione ed in particolare assicurarsi sempre che non vengano dimenticati sulle postazioni (server e client) oggetto di intervento;
- **evitare** di fare o di richiedere copie di dati personali se non necessario;
- **cancellare** le copie di dati personali, su supporti rimovibili, che non siano più necessarie per finalità di manutenzione e assistenza tecnica;
- **provvedere** alla distruzione dei dischi non riscrivibili che contengano dati personali sensibili o giudiziari che non sia necessario detenere o utilizzare;
- **prelevare** dalle apparecchiature informatiche o elettromedicali da dismettere tutti i supporti di memoria provvedendo, se autorizzato, alla loro distruzione controllata.

Istruzioni per i Responsabili e gli Incaricati per il corretto trattamento dei dati su supporto cartaceo : cartelle cliniche e documentazione sanitaria(1)

I documenti sanitari contengono dati personali,ascrivibili alla categoria dei dati sensibili, in quanto idonei a rilevare lo stato di salute o la vita sessuale degli interessati; per il loro trattamento da parte gli organismi sanitari ed esercenti le professioni sanitarie pubblici e privati il Codice Privacy prevede, l'adozione di misure di sicurezza e accorgimenti particolari.

1) non rilevare sul frontespizio alcun dato personale sensibile;
2) i documenti contenenti dati personali di natura sensibile devono essere custoditi in stanze o locali, o armadi o carrelli chiusi a chiave e le chiavi devono essere custodite da personale autorizzato (accesso selezionato) e va redatto dal Responsabile della U.O. di appartenenza un registro ed un verbale di consegna delle chiavi; il personale Incaricato del trattamento deve verificare che detti locali o armadi contenenti i documenti siano chiusi a chiave;
3) quando le cartelle cliniche o altra documentazione contenente dati idonei a rivelare lo stato di salute sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, oppure devono essere trasferite da una struttura o da un ufficio presso altro luogo (esempio archivio di deposito) è necessario che i medesimi atti e documenti siano controllati e custoditi dagli Incaricati e che questi utilizzino ogni cautela per la protezione della riservatezza al fine di impedire che ad essi accedano persone prive di autorizzazione, fino alla restituzione, cioè al termine delle operazioni affidate;
4) si consiglia di inserire la documentazione in busta chiusa o in raccoglitori sigillati sui quali apporre la propria firma per garantirne l'integrità;
5) evitare di scrivere dati personali di natura sensibile su lavagne o altri supporti che possano essere visionati da persone non autorizzate;
6) 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);
7) 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.

(1)Sono considerati documenti sanitari e sono oggetto della disciplina del presente manuale i seguenti documenti:
1. cartelle cliniche;
2. schede di accettazione/dimissione ospedaliere;
3. lastre radiologiche;
4. referti diagnostici;
5. referti analitici;
6. verbali relativi a prestazioni di pronto soccorso;
7. certificazioni sanitarie riguardanti pazienti assistiti in ospedale;
8. registri operatori e registri nosologici di reparto;
9. certificazioni relative a pazienti trattati in sede ambulatoriale;
10. esiti degli accertamenti di carattere sanitario compiuti dagli organi ispettivi del servizio di igiene pubblica, ambientale e tutela della salute nei luoghi di lavoro;
11. ogni altro tipo di documentazione che contenga riferimenti o anamnesi, referti, diagnosi, lesioni, patologie o qualsiasi altro elemento idoneo a rilevare lo stato di salute di una persona.

Sicurezza per la privacy degli archivi cartacei.

L'assegnazione degli spazi di lavoro deve avvenire secondo criteri tali da impedire la promiscuità di permanenza e di utilizzazione tra:

- personale incaricato del trattamento di dati personali;
- personale non incaricato di trattamento di dati personali;
- soggetti estranei all'azienda

Il personale dipendente incaricato di trattamento ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:

- la necessità di trattamento;
- il minimo livello di conoscenza dei dati.

I Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari. E' altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi.

Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato, ivi compresi i locali destinati al personale addetto alla video sorveglianza;
- ostacolare l'accesso abusivo ai dati;
- segnalare la presenza di intrusi;
- l'accesso agli archivi, sia operativi che remoti, contenenti dati sensibili o giudiziari, deve
- essere controllato e permesso unicamente agli Incaricati del trattamento e la protezione dei dati
- deve essere incentrata alla sicurezza per la privacy degli archivi stessi;
- va redatto, ad opera del Responsabile, un elenco del personale Incaricato che detiene le chiavi di detti archivi;
- l'accesso di persone non autorizzate (es. pazienti/utenti) deve essere vietato ai locali dove i documenti sono presenti senza il presidio di un Incaricato;
- l'accesso agli archivi aziendali deve essere controllato e devono essere identificati e registrati i soggetti che vi sono ammessi.
- 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.
- le risorse dei fornitori esterni che per esigenze di lavoro accedono ai locali ove sono presenti documenti contenenti dati sensibili o giudiziari, fuori dall'orario di lavoro (es. addetti alla pulizie/manutenzione), devono essere identificate in un allegato al contratto di fornitura;
- i documenti contenenti dati sensibili o giudiziari devono essere utilizzati dagli Incaricati del trattamento solo per il tempo necessario allo svolgimento dei relativi compiti e poi riposti negli archivi;
- gli incaricati devono custodire i documenti in maniera che ad essi non accedano persone prive di autorizzazione (es. mai lasciare incustoditi i documenti durante il loro trattamento);
- custodire le fotocopie (autorizzate) con le stesse modalità degli originali;
- la consegna dei documenti (es. referti) deve prevedere l'identificazione dell'Interessato o di un suo delegato e sarà eseguita in busta chiusa.
- i trasferimenti di documenti tra uffici interni deve prevedere l'utilizzo di buste sigillate o altre precauzioni che impediscano la consultazione degli stessi da parte di persone non autorizzate;

- tutti i documenti non più necessari devono essere resi inutilizzabili, distrutti, resi illeggibili prima di essere cestinati (è necessario fare ricorso ai distruggi documenti: carta, CD, DVD).

Il Responsabile degli archivi cartacei (ossia il Direttore Sanitario) dovrà curarne la custodia in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati personali contenuti nei documenti archiviati.

LE REGOLE DI ORDINARIA DILIGENZA

Nell'esecuzione dei compiti assegnati il dipendente, Responsabile o Incaricato, deve attenersi ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento.

Per queste ragioni il dipendente , nello svolgimento delle proprie mansioni deve prestare particolare attenzione nel:

• non divulgare a terzi estranei le informazioni di cui viene a conoscenza;

• adoperarsi affinché terzi fraudolentamennte non entrino in possesso di dati deliberatamente comunicati

• non fare copie, per uso personale, dei dati su cui svolgono operazioni di ufficio;

• attenersi scrupolosamente alle istruzioni impartite dai Responsabili;

• osservare i criteri di riservatezza;

• trattare i dati in modo lecito e secondo correttezza;

• trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;

• comportarsi 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;

• qualora l'Incaricato **abbandoni temporaneamente** la propria postazione di lavoro deve provvedere a :

a) fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.

b) riporre nei cassetti o negli armadi la documentazione cartacea contenente dati personali.

c) Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salva schermo del PC con password

d) Non rivelare o fare digitare le password dal personale di assistenza tecnica.

e) Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle.

f) Segnalare qualsiasi anomalia o stranezza al Responsabile e/o al Titolare .

Sanzioni per inosservanza delle norme

Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta. **Riportiamo di seguito un riassunto delle principali norme in materia.**

Gli illeciti penali

Trattamento illecito di dati (Art. 167 Codice privacy)	Salvo che il fatto non costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione della normativa è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a tre anni. Tale articolo ha una vasta applicazione. Soprattutto, tale articolo è specificamente applicabile nei casi di mancato ottenimento del consenso scritto.
Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168 Codice privacy)	Chiunque, nella notificazione o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
Misure di sicurezza (Art. 169 Codice privacy)	Chiunque, essendovi tenuto, omette di adottare le misure minime previste è punito con l'arresto sino a due anni o con l'ammenda da 10.000 a 50.000 Euro. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario. (…) Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.

Inosservanza di provvedimenti del Garante (Art. 170 Codice privacy)	Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante, è punito con la reclusione da tre mesi a due anni.

Le violazioni amministrative

Omessa o inidonea informativa all'interessato (Art.161 Codice privacy)	Sanzioni da 3000 a 18000 Euro, oppure da 5.000 a 30.000 Euro se dati sensibili. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.
Omessa o incompleta notificazione (Art. 163 Codice privacy)	Sanzioni da 10.000 Euro a 60.000 Euro ed in più condanna alla pubblicazione della sentenza.
Omessa informazione o esibizione al Garante (Art. 164 Codice privacy)	Sanzioni da 4.000 a 24.000 Euro.
Cessione illecita di dati ("Altre fattispecie", Art. 162 Codice privacy)	La cessione dei dati in violazione della normativa sul trattamento di dati personali è punita con la sanzione amministrativa da 5.000 a 30.000 Euro.
Pubblicazione della sentenza ("Pene accessorie", Art. 172 Codice privacy)	La condanna per uno dei delitti previsti dal Codice importa la pubblicazione della sentenza.

La responsabilità civile per danni

Danni cagionati per effetto del trattamento (Art. 15 Codice privacy)	Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. E' risarcibile anche il danno non patrimoniale.

Norme di rinvio

Per tutto quanto non espressamente previsto dal presente regolamento, si applicano le disposizioni previste dal Decreto Legislativo n. 196 del 30 giugno 2003, novellato "Codice in materia di protezione dei dati personali", la normativa vigente, le altre disposizioni legislative comunque attinenti ed i provvedimenti del Garante in materia.