Azienda Sanitaria Regionale Molise

ASREM

REGOLAMENTO AZIENDALE

attuativo delle disposizioni di cui al D.Lgs 30 giugno n.196/2003
"Codice in materia di protezione dei dati personali".

Articolo 1 - Oggetto e finalità

Il presente regolamento disciplina all'interno della ASReM, di seguito denominata Azienda, la tutela delle persone e degli altri soggetti in ordine al trattamento dei dati personali nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali emanato con D.Lgs. 30 giugno 2003 n. 196, di seguito denominato "Codice Privacy" o semplicemente "Codice". Le prescrizioni in esso contenute devono intendersi come istruzioni impartite dal Titolare del trattamento ai sensi dell'art. 29 comma 5 del Codice Privacy volte a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali degli utenti e di tutti coloro che hanno rapporto con l'Azienda.

1.1- ***Norme di rinvio***

Per tutte le definizioni si fa riferimento a quelle contenute nel Codice Privacy, con particolare riferimento all'art. 4, nonché ai contenuti dei Provvedimenti Generali emanati dall'Autorità Garante per la Protezione dei dati personali.

Per tutti i principi generali e particolari si fa riferimento a quelli contenuti nel Codice Privacy nonché ai contenuti dei Provvedimenti Generali ed alle Autorizzazioni Generali emanati dall'Autorità Garante per la Protezione dei dati personali.

Articolo 2 - Organigramma privacy

L'Azienda – Titolare dei trattamenti di dati personali – ha individuato la propria struttura di presidio privacy con Provvedimento del Direttore Generale n. 927 del 12.08.2010 (Modello organizzativo ed individuazione dei soggetti competenti in materia di protezione dei dati personali) e successiva integrazione adottata con Provvedimento del Direttore Generale n. 1052 del 29.07.2011 (Integrazione Provvedimento n. 927 del 12.08.2010 - Modello organizzativo ed individuazione dei soggetti competenti in materia di protezione dei dati personali).

Inoltre, con riferimento a partner esterni all'Azienda, concorre a definire la struttura di presidio privacy, il Provvedimento del Direttore Generale n. 360 del 17 aprile 2008 (Approvazione di schemi-tipo relativi a protocolli d'intesa operativi inerenti la gestione e lo scambio di dati personali per la realizzazione di finalità istituzionali).

2.1 - ***Titolare del trattamento***

Il *Titolare* del trattamento dei dati personal,i ai sensi dell' art. 28 del Codice, è l'Azienda nel suo complesso rappresentata dal Direttore Generale in qualità di Legale rappresentante dell'Azienda stessa.

Il *Titolare* provvede, tra l'altro:

- ad assolvere all'obbligo di notificazione al Garante per la protezione dei dati personali (di seguito indicato Garante), nonché delle comunicazioni al Garante stesso previste dall'art.39, comma 1, del Codice;
- a richiedere al Garante l'autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa;
- a nominare, con proprio atto, i *Responsabili* del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice, all'adozione di misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a nominare il dirigente aziendale privacy (di seguito indicato *Referente privacy*) e l'*Amministratore di sistema*;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.

2.2 - ***Responsabili del trattamento***

Il '*Responsabile' del trattamento* è il soggetto, designato per iscritto dal *Titolare*, che, ai sensi dell'art. 29 del Codice possa garantire per esperienza, capacità ed affidabilità, il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Ogni *Responsabile* deve garantire:

- il tempestivo ed integrale rispetto delle norme contenute nel Codice, delle disposizioni del Garante, delle disposizioni contenute nei provvedimenti del D.G. e nel presente Regolamento, nonché della normativa nazionale e regionale che disciplina specifici trattamenti dei dati, con particolare riguardo:
  - all'art. 5 della legge n. 135/1990 per la tutela della riservatezza della persona affetta da infezione HIV;
  - alla legge n. 194/1978 per le comunicazioni sulle interruzioni di gravidanza;
  - agli art. 120-121 del DPR n. 309/1990 in materia di tossicodipendenza;

- agli art. 5-5bis della Legge n. 94/1998 in materia di sperimentazione clinica in campo oncologico;
- all'art. 734 bis del C.P. circa il divieto di divulgazione non consentita dell'immagine delle persone offese da atti di violenza sessuale.

- l'adozione di idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente e dai Regolamenti e/o provvedimenti adottati a livello aziendale.
- una fattiva collaborazione con il *Referente Privacy* provvedendo a:
- fornire le informazioni richieste
- comunicare tempestivamente tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
- comunicare i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento dell'anagrafe aziendale dei trattamenti.

In particolare deve:

- operare in modo che siano ridotti al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- designare i soggetti '*incaricati*', definendone livelli di autorizzazione all'accesso ai dati e modalità di esecuzione delle attività demandate e formalizzandone ruolo e responsabilità ai sensi della disciplina vigente; la designazione degli *incaricati* va effettuata nei servizi relativamente ai quali l'Azienda non vi abbia provveduto tramite preventiva individuazione degli ambiti di trattamento consentiti;
- curare che ai soggetti interessati (ovvero a coloro i cui dati vengono trattati nell'ambito della funzione di Responsabile dei Trattamenti) venga erogata l'informativa prevista secondo i modelli forniti dall'Azienda e che da parte degli stessi venga acquisito il consenso al trattamento nei casi previsti;
- avvertire immediatamente il *Titolare* di ogni richiesta, provvedimento, accertamento, controllo da parte del Garante o dell'Autorità giudiziaria.

Il *Responsabile* del trattamento risponde al *Titolare* per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al proprio settore di competenza.

La funzione di *Responsabile* non è delegabile. In caso di assenza o impedimento del *Responsabile* del trattamento le relative attribuzioni sono esercitate da chi lo sostituisce per le attività di istituto.

2.3 - ***Responsabili interni***

Avvalendosi delle previsioni di cui all'art. 29 del Codice, il Titolare ha individuato quali *Responsabili dei Trattamenti* i Dirigenti Responsabili pro-tempore di strutture organizzative (UOC, UOS) nonché ulteriori eventuali soggetti, anche diversi da quelli specificati al punto 3 del provvedimento D.G. 927/2010 (quali il Medico Competente), deputati a svolgere all'interno di alcune Strutture, Dipartimenti e/o Servizi (non strutturati in Unità Operative) un ruolo diverso da quello individuato nello stesso provvedimento che hanno comunque accesso, per dovere d'ufficio, a dati personali e sensibili di dipendenti e/o utenti per la sicurezza dei quali sussistano particolari esigenze di controllo, sempreché i soggetti individuati posseggano i requisiti presupposti dall'art. 29 del Codice Privacy.

All'atto del conferimento dell'incarico di Responsabile di U.O., il provvedimento disposto dal D.G. deve contenere la formale designazione a "R*esponsabile del trattamento"* che verrà successivamente formalizzata allegando al contratto l'atto di nomina (*ALL. 1*), conformemente allo schema tipo approvato con il provvedimento del D.G. n. 927/2010.

Anche il dipendente che svolge attività libero-professionale intra-moenia in locali messi a disposizione dall'Azienda, è individuato quale *Responsabile del trattamento* dei dati effettuati in tale attività. Il Responsabile della struttura competente in merito alla gestione dell'attività libera professionale intra-moenia, deve inserire nell'atto di autorizzazione a tale attività, la nomina a *responsabile del trattamento* del dipendente interessato, a cui è fatto carico di nominare eventuale *incaricati*.

Il Responsabile dell'U.O.C. "Risorse Umane" deve trasmettere al *Referente Privacy* copia dell'atto di nomina a "*Responsabile*" del trattamento, debitamente sottoscritto, e comunicare qualsiasi intervenuta modifica nell'affidamento di incarichi di Responsabilità dei ruoli sanitario, amministrativo e tecnico al fine di consentire l'aggiornamento costante dell'elenco dei *Responsabili* del trattamento.

2.4 - ***Responsabili esterni***

Il Titolare del trattamento, al punto 4 del provvedimento D.G. 927/2010, ha individuato quali "*Responsabili del trattamento dei dati personali*" anche i soggetti esterni che, in qualità di appaltatori o contraenti, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle dell'Azienda, con rilevante attività di trattamenti di dati Personali di competenza

aziendale (ad esempio: fornitura di procedure complesse anche di natura informatica, di prestazioni professionali o di prestazioni e servizi anche in convenzione).

Tali soggetti che, per esigenze organizzative dell'Azienda, effettuano trattamenti di dati per conto di quest'ultima con utilizzazione della propria organizzazione e di quella dell'Azienda stessa (ad esempio: società di informatica, enti, soggetti accreditati, associazioni di volontariato e simili, consulenti, istituti di credito ed assicurativi,ecc.), sono nominati "*Responsabili esterni"* del trattamento, sempreché in possesso dei requisiti previsti dall'art. 29 comma 1 del Codice (esperienza, capacità, affidabilità).

Il Dirigente Responsabile della Struttura correlata al Servizio/attività "esternalizzata," dovrà proporre al *Titolare* la nomina di *Responsabile del trattamento* in capo al soggetto esterno. Qualora la nomina non venisse proposta, la "responsabilità del trattamento" resta – rationae materiae – in capo al Dirigente Responsabile.

L'obbligo del concorrente di accettare, in caso di aggiudicazione del Servizio/attività "esternalizzata", senza alcun onere aggiuntivo a carico della stessa - il ruolo di *Responsabile esterno* del trattamento dei dati personali (come individuato all'art. 29 del Codice Privacy), ovvero, a sottoscrivere specifico protocollo d'intesa circa le modalità del trattamento dei dati personali il cui schema è allegato al Provvedimento del D.G. n. 360/2008 (Approvazione di schemi-tipo relativi a protocolli d'intesa operativi inerenti la gestione e lo scambio di dati personali per la realizzazione di finalità istituzionali), deve essere previsto negli atti di gara (capitolati, lettere di invito, ecc.) dai Responsabili delle Strutture che attivano le procedure negoziate.

Al momento dell'affidamento del servizio, il relativo contratto da stipulare tra l'Azienda e l'Impresa aggiudicataria, deve prevedere, in una apposita clausola (*ALL. 2*), il ruolo che l'Impresa medesima - a discrezione dell'Ente, su proposta del Dirigente Responsabile del Servizio - ha assunto, in relazione al trattamento dei dati personali, con la sottoscrizione dell'atto di nomina di *Responsabile esterno del trattamento* o del Protocollo d'intesa.

Copia dell'atto di nomina *(ALL. 3)* o del Protocollo d'intesa *(ALL. 4),* proposto dal Dirigente Responsabile del Servizio, sottoscritto dal *Titolare del* trattamento e controfirmato dal Legale rappresentante dell'Impresa, deve essere trasmesso dai Responsabili delle Strutture competenti per la stipula degli accordi, convenzioni e contratti, al *Referente Privacy*.

I Responsabili delle strutture sopraindicate devono procedere ad una ricognizione dei contratti stipulati dall'Azienda, al fine di provvedere all'eventuale designazione dei *Responsabili esterni.*

I *Responsabili esterni* hanno l'obbligo:

- di trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;

- di rispettare le misure di sicurezza previste dal Codice sulla privacy e di adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- di nominare al loro interno i soggetti *incaricati* del trattamento;
- di garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
- di trattare i dati personali, anche di natura sensibile e sanitaria, dei pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione;
- di attenersi alle disposizioni impartite dal *Titolare* del trattamento;
- di specificare i luoghi dove fisicamente avviene il trattamento dei dati.
- di relazionare annualmente sulle misure di sicurezza adottate;
- di allertare immediatamente il *Titolare* in caso di situazioni anomale di emergenza.

Nel caso di mancato rispetto delle predette disposizioni, i *Responsabili esterni* del trattamento devono intendersi autonomi "*Titolari*" del trattamento e quindi, soggetti ai rispettivi obblighi e, pertanto, rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

2.5 - ***Incaricati del trattamento interni***

Ai sensi dell' art. 30 - comma 1- del Codice Privacy, sono *incaricati* del trattamento le persone fisiche autorizzate a compiere operazioni di trattamento dal *Titolare* o dal *Responsabile*, attenendosi alle istruzioni impartite. La designazione è fatta per iscritto.

L'Azienda, come contemplato dall'art. 30 comma 2, ha individuato previamente per le UU.OO. e/o i Servizi aziendali, gli ambiti di trattamento consentiti a tutte le categorie di operatori (sanitario, amministrativo, ecc.), così da designare implicitamente gli stessi quali "*incaricati* dei trattamenti" contestualmente alla loro preposizione alla specifica attività a loro attribuita all'interno delle UU.OO. e/o dei Servizi;

I *Responsabili* dei Trattamenti hanno comunque, la facoltà di fornire per iscritto ulteriori istruzioni agli *incaricati*, nonché di fornire ulteriori istruzioni per il trattamento di dati personali o dettagliarne gli ambiti o integrare o modificare i profili previamente individuati, qualora ciò sia richiesto da specificità o comunque, sia necessario per garantire maggior livello di sicurezza dei dati.

Gli *incaricati* hanno accesso ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali loro assegnati.

In particolare, l'*Incaricato* deve assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito e secondo correttezza;

- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con questi scopi;
- esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti e, se dati sensibili, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

L'*Incaricato* è tenuto alla completa riservatezza sui dati di cui sia venuto a conoscenza in occasione dell'espletamento della sua attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal *Titolare* e dal *Responsabile*, nei soli casi previsti dalla legge e/o nello svolgimento dell'attività istituzionale dell'Azienda.

Durante il trattamento in caso di allontanamento dal posto di lavoro, l'incaricato deve adottare le misure previste e a sua disposizione secondo le istruzioni ricevute dal *Responsabile* del trattamento contemplate nel manuale "*Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i.* redatto dalla Struttura privacy aziendale, per evitare l'accesso non autorizzato da parte di terzi, anche se dipendenti, ai dati personali trattati o in trattamento.

2.6 - ***Incaricati esterni del trattamento che operano all'interno dell'azienda***

Tutte le persone che prestano attività all'interno dell'Azienda stessa a qualsiasi titolo, con o senza retribuzione, compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dall'Azienda sono tenuti al rispetto di quanto previsto dal presente regolamento e, in particolare:

- ad attenersi alla massima riservatezza rispetto alle notizie ed alle informazioni di cui vengono a conoscenza;
- ad attenersi alle operazioni di trattamento loro consentite per i relativi ambiti di trattamento o/e alle eventuali ulteriori istruzioni fornite per iscritto dal *Responsabile* del trattamento.

La designazione viene effettuata ai sensi dell' art. 30 - comma 2- del Codice Privacy.

2.7 - ***Referente aziendale per la Privacy***

Al fine di garantire una efficace applicazione delle disposizioni sulla Privacy, il Direttore Generale, *Titolare* del trattamento, ha attribuito al dirigente aziendale privacy (*referente Privacy*), le seguenti funzioni:

- supporto alla Direzione Generale per l'adozione di misure idonee di sicurezza, anche preventive, volte a garantire la privatezza, l'integrità, la disponibilità e l'autenticità dei dati gestiti;
- supporto alla Direzione Generale per l'applicazione della normativa privacy e per formulare proposte per facilitare l'esercizio dei diritti dell'interessato ex art. 7 del D.Lgs. n. 196/2003;
- supporto ai *Responsabili* del trattamento negli adempimenti previsti dalla normativa privacy;
- verifica periodica sull'attività dei *Responsabili* del Trattamento rispetto alle istruzioni impartite dal *Titolare* del trattamento;
- controllo e coordinamento dell'attività dell'*Amministratore di sistema*.

Nell'esercizio delle competenze di cui sopra, deve essere garantita al *Referente privacy* la collaborazione di tutte le articolazioni organizzative dell'Azienda e, in particolare, dei Direttori dei Presidi Ospedalieri, dei Distretti socio-sanitari, delle UU.OO. Sovradistrettuali, dei Dipartimenti di Prevenzione e Protezione e di Salute Mentale, come disposto dal *Titolare del trattamento*, al punto 7 del provvedimento D.G. 927/2010.

Gli stessi soggetti, ovvero i funzionari da loro individuati e delegati a tale attività, supportano il Referente Privacy, in particolare:

- nell'analisi delle problematiche indicate dai Responsabili delle UU.OO. strettamente correlate al trattamento e alla protezione dei dati sensibili trattati dagli operatori (sanitari, amministrativi, ecc.) nelle relative strutture di appartenenza;
- nella segnalazione di eventuali criticità;
- nella formulazione di proposte operative riguardanti la sicurezza aziendale.

2.8 - ***Amministratori di sistema***

Il *Titolare del trattamento*, al punto 5 del provvedimento D.G. 927/2010, ha individuato - in esecuzione del Provvedimento Generale del Garante del 27/11/2008 - la funzione dell'*Amministratore di sistema interno"* per gli adempimenti delle attività previste dal Disciplinare Tecnico (Allegato B del d.Lgs. 196/2003), non espletate da Ditte esterne, da attribuire ad un soggetto interno all'organizzazione aziendale, di provata esperienza, capacità ed affidabilità, atto a garantire il rispetto delle disposizioni in materia di protezione dei dati personali, sotto il profilo della sicurezza e specificatamente di quella informatica.

All'*Amministratore di Sistema interno*, è delegata (provvedimento del D.G. n.1686/ 2010) l'attività di gestione tecnica del sistema informatico finalizzata alla sicurezza del trattamento dei dati mediante strumenti elettronici che si concretizza:

- nel garantire la sicurezza dei database in conformità delle prescrizioni del D.Lgs.196/03 e s.m.i. e del disciplinare tecnico all. B;
- nella predisposizione di idonee e preventive misure di sicurezza informatiche

e, in dettaglio, nei compiti e responsabilità indicate nel modello di nomina allegato al citato provvedimento.

L'*Amministratore interno* deve coadiuvare i *Responsabili del trattamento* nell'individuazione ed applicazione delle misure, sia minime che idonee, volte alla protezione dei dati trattati in Azienda, per quanto di sua competenza, e collaborare fattivamente con il *referente privacy* per l'attuazione delle prescrizioni impartite dal Garante.

Nel caso che la gestione dei sistemi informatici sia affidata a Ditte esterne - così come prefigurato dal provvedimento generale del garante per la protezione dei dati personali datato 27/11/2008: "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema" e s.m.i. - è fatto obbligo alle Ditte medesime, sulla base di espressa clausola contrattuale da prevedere nel bando di gara (*ALL.5*), di assumere le funzioni di *amministratore di sistema*, senza alcun onere aggiuntivo a carico dell'Azienda.

L'elenco dei nominativi preposti alle specifiche funzioni deve essere comunicato dalle Ditte esterne al Dirigente Responsabile del Servizio che provvede a inoltrarle all'*Amministratore di Sistema* e al *Referente privacy*.

I Responsabili delle strutture affidatarie di prestazioni di servizi in materia informatica devono fornire informazioni all'*Amministratore di Sistema interno* sui contratti in essere per consentire allo stesso la formalizzazione delle designazioni ai soggetti esterni individuati *Amministratore di sistema*, dandone contestuale comunicazione al *Referente Privacy*.

2.9 - ***Diritti dell'interessato***

L'interessato è il soggetto, persona fisica, persona giuridica, ente o associazione, al quale si riferiscono i dati oggetto del trattamento. L'Azienda attua tutte le misure necessarie a facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 7 del Codice Privacy.

A tal fine il Codice sulla privacy prevede che l'interessato, con richiesta fatta senza formalità, ha diritto di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati;
- la comunicazione dei dati che lo riguardano in forma comprensibile (anche attraverso l'utilizzo di una grafia leggibile; in caso di comunicazione di codici o sigle sono forniti i parametri per la comprensione del relativo significato);
- l'indicazione:

• dell'origine dei dati personali;

- delle finalità e modalità del trattamento;
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- degli estremi identificativi del titolare e dei responsabili;
- dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;

- l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'attestazione che le operazioni di cui ai punti 4 e 5 sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano ai fini di invio di materiale informativo o di comunicazione istituzionale.

Articolo 3 - Il trattamento dei dati

Con l'espressione "*trattamento*", ai sensi dell'art. 4 del Codice, deve intendersi qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici, concernenti:

- la raccolta dei dati;
- la registrazione dei dati, cioè il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.;
- la conservazione dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la consultazione;
- l'elaborazione, ovvero le operazioni che attribuiscono significato ai dati in relazione allo scopo per i quali essi sono stati raccolti;
- la modificazione dei dati registrati in relazione a variazioni o a nuove acquisizioni

- la selezione, l'estrazione, e il raffronto, ipotesi specifiche che rientrano nell'ipotesi più generale dell'elaborazione;
- l'utilizzo;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la comunicazione, ovvero la trasmissione dei dati ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; non è comunicazione la trasmissione dei dati allo stesso interessato, al Responsabile e agli Incaricati del trattamento;
- la diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es.: pubblicazione all'albo, giornale, ecc.);
- la cancellazione;
- la distruzione.

Articolo 4 - Principi fondamentali del trattamento dei dati

I dati personali oggetto del trattamento devono essere:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti, e se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti.

Articolo 5 - Conservazione e sicurezza dei dati

Per il trattamento dei dati personali, l'Azienda, adotta misure di sicurezza, fisiche, logiche ed organizzative, al fine di garantire l'integrità, la disponibilità e la protezione dei dati stessi e di ridurne al minimo i rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Per la realizzazione delle finalità di cui al comma 1, si provvede con:
- l'adozione, di linee-guida per dare piena applicazione alle misure minime di sicurezza previste dal Codice;

- la verifica, a cura dei Responsabili del trattamento in collaborazione con l'Amministratore di sistema, dell'applicazione delle misure di sicurezza stabilite.

Articolo 6 - Censimento dei Trattamenti dei Dati

I trattamenti effettuati dall'Azienda sono finalizzati all'erogazione delle prestazioni sanitarie nonché agli adempimenti amministrativi e contabili, di organizzazione e di controllo preordinati alla predetta erogazione, con particolare riguardo alle attività di:

- prevenzione collettiva e di sanità pubblica svolte dal Dipartimento di Prevenzione, anche a supporto delle autorità sanitarie;
- diagnostica strumentale e di laboratorio;
- prevenzione delle malattie, cura e riabilitazione in regime ambulatoriale sia in sede distrettuale che ospedaliera;
- ricovero ordinario e in day hospital;
- ricovero in regime residenziale e semiresidenziale;
- prestazioni sanitarie a rilevanza sociale;
- attività o servizi socio-assistenziali su delega dei singoli enti locali;
- medicina legale;
- ricerca e sperimentazione, nonché elaborazione statistica, epidemiologica e sociologica;
- controllo della salute dei lavoratori che operano all'interno dell'Azienda.

Sono altresì effettuati i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti:

- la gestione del personale dipendente, ivi comprese le procedure di assunzione;
- la gestione dei soggetti, che intrattengono rapporti giuridici con l'Azienda, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
- la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni di servizi nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
- la gestione dei rapporti con i soggetti accreditati o convenzionati;
- la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Le banche dati relative ai dati trattati vengono periodicamente censite e aggiornate, attraverso richiesta ai *Responsabili del trattamento*, che dovranno comunicare l'elenco dei trattamenti dati effettuati nell'ambito della propria struttura.

Articolo 7 - Modalità di trattamento dei dati

Le modalità di trattamento dei dati sono quelle indicate nel Codice. Il trattamento può avvenire con o senza strumenti elettronici. Il *Responsabile del trattamento* è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. I *Respons*a*bili* curano la diffusione delle istruzioni per il corretto trattamento dei dati, contenute nel manuale "*Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i.*, , precisandole, ove occorra, in forma scritta.

7.1 - ***Trattamento dei dati senza l'ausilio di macchine e strumenti elettronici***

Nel trattamento dei dati senza l'ausilio di strumenti elettronici, quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. Tutta la documentazione contente dati personali deve essere custodita in armadi dotati di serratura, le cui chiavi devono essere conservate in modo appropriato o, altrimenti con altre modalità tali da impedire l'accesso a terzi non autorizzati (ad esempio, chiudendo la porta della stanza in cui si trova la documentazione, qualora non sia presente alcun incaricato che possa garantirne la sicurezza). L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione in occasione della consultazione di documenti di altro genere.

Per quanto afferisce al periodo di conservazione dei documenti (art. 11 comma 1, lettera e) del Codice, l'Azienda ha adottato un apposito regolamento interno, con provvedimento del D.G. n. 628/2007.

I *Responsabili dei Trattamenti* devono provvedere annualmente all'individuazione dei documenti da scartare attivando le procedure di tutela nei confronti delle competenti autorità, con particolare riferimento alla Sovrintendenza Archivistica.

7.2 - ***Trattamento dei dati con l'ausilio di macchine e strumenti elettronici***

I *Responsabili dei Trattamenti*, per contribuire a garantire la sicurezza informatica di tutta l'Azienda, sono tenuti a dare istruzioni specifiche agli incaricati sul corretto utilizzo degli strumenti elettronici e informatici (fotocopiatori, stampanti, fax, telefono, computer, internet e posta elettronica, ecc.), conformemente a quanto indicato, nel *Regolamento Aziendale per l'utilizzo delle postazioni di informatica individuale, di utilizzo della posta elettronica e della rete Internet aziendale* approvato con provvedimento del D.G. n. 1627/2009, e nel manuale "*Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i.*," distribuito dalla Struttura Privacy a ciascuna Struttura aziendale.

7.3 - ***Uso delle apparecchiature di videosorveglianza***

L'installazione di apparecchiature di videosorveglianza è autorizzata dal *Titolare del trattamento* solo quando ciò sia strettamente indispensabile per l'esercizio delle attività assistenziali, ovvero per la sicurezza delle persone e delle attrezzature (monitoraggio delle persone ricoverate, controlli di corridoi, di sale di attesa o di atri locali, di spazi esterni, delle porte di accesso agli edifici) e non sono attuabili o sufficienti altre misure di sorveglianza.
Il trattamento dei dati con le suddette apparecchiature è effettuato nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori e delle prescrizioni del Garante contenute nel Decalogo sulla Videosorveglianza (Provvedimento generale del Garante dell'8 aprile 2010).
I Responsabili di servizio che intendono avvalersi di sistemi di videosorveglianza possono richiedere un preventivo parere al *Referente Privacy*.

Art. 8 - Il trattamento dei dati personali ordinari

Il trattamento dei dati personali ordinari da parte dell'Azienda, in quanto soggetto pubblico, è consentito solo per lo svolgimento delle funzioni istituzionali. La comunicazione dei dati personali ad un altro soggetto pubblico è ammessa quando è prevista da una norma di legge o di regolamento o, in mancanza, quando è necessaria per lo svolgimento delle funzioni istituzionali. In quest'ultima ipotesi la comunicazione non può essere effettuata se non dopo il decorso del termine di cui all'art. 39, comma 2 del Codice. La comunicazione a soggetto privato è ammessa soltanto quando è prevista da una norma di legge o regolamento.

Articolo 9 - Il trattamento dei dati sensibili e giudiziari

L'Azienda in quanto soggetto pubblico, può trattare i dati sensibili, che non siano di natura sanitaria, e i dati giudiziari, solo quando il trattamento è autorizzato da espressa disposizione di legge.
Le regole per il trattamento di dati sensibili e giudiziari da parte di soggetti pubblici sono contenute negli art. 20 (dati sensibili) e 21 (dati giudiziari) del Codice. In ogni ipotesi di trattamento dei dati sensibili e giudiziari occorre verificare, sia preliminarmente sia durante il trattamento, che i dati trattati siano indispensabili per svolgere le attività istituzionali e non sia possibile utilizzare solo dati anonimi. Tale trattamento deve essere effettuato in modo da prevenire la violazione dei diritti, delle libertà fondamentali e della dignità delle persone.
Il trattamento è ammesso solo in presenza di rilevante finalità di interesse pubblico perseguito, e se sono ben definiti – caso per caso – quali sono i tipi di dati trattati e quali le operazione eseguite: tali presupposti debbono essere contenuti in una 'espressa disposizione di legge'; in assenza di tale previsione, ciascuna pubblica amministrazione deve dotarsi di un Regolamento contenente tutti i presupposti suindicati che sia stato previamente assentito dal Garante.
L'Azienda, non potendo, per legge, adottare un regolamento di questo tipo, si impegna a recepire ed applicare al suo interno il regolamento sui dati sensibili e giudiziari predisposto dalle Amministrazioni dotate di potere regolamentare generale, a livello nazionale o regionale.

9.1 - *Comunicazione e diffusione*

Particolare attenzione deve essere prestata da tutti gli operatori qualora le operazioni di trattamento, note come comunicazione e diffusione, coinvolgano i dati sensibili e giudiziari. La comunicazione e diffusione dei dati è possibile a condizione che le stesse trovino copertura normativa in disposizioni legislative, o in mancanza, nel Regolamento regionale, fermo restando che i dati idonei a rivelare lo stato di salute non possono essere mai diffusi. Nel casi dubbi, è indispensabile consultare il Regolamento Regionale che si compone di 'schede' grossomodo coincidenti con le attività enucleate tra quelle costituenti i livelli essenziali di assistenza, in quanto la comunicazione e diffusione dei dati sono due tra le possibili operazioni che costituiscono trattamento di dati personali, e pertanto legittime solo se previste nel Regolamento.

9.2 - *Comunicazione di dati all'interessato relativi allo stato di salute*

La comunicazione e le informazioni sullo stato di salute e sulle specifiche patologie dell'interessato possono essere rese a quest'ultimo solo per il tramite di un medico. In subordine, la comunicazione può avvenire da parte di esercenti le professioni sanitarie diversi dai medici che nell'esercizio dei

propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute solo se autorizzati per iscritto. L'atto di incarico deve individuare appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

ARTICOLO 10 - Informativa e Consenso

Per qualsiasi trattamento di dati personali è indispensabile 'informare' l'interessato (ovvero il soggetto di cui si trattano i dati) e, solo per i trattamenti di dati sensibili finalizzati alla tutela della salute o dell'incolumità fisica dell'interessato, occorre acquisire il consenso al trattamento dei dati personali.

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.

L'Azienda, mediante le proprie strutture, si avvale della facoltà di fornire un'unica informativa per la pluralità dei trattamenti di dati effettuati, anche ai fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi. L'informativa è fornita per iscritto, attraverso stampati ed è *integrata da appositi e idonei cartelli agevolmente visibili dal pubblico, affissi nei locali di accesso dell'utenza* e pubblicata su sito internet istituzionale.

L'informativa, approvata con provvedimento del D.G. n. 1251 del 27 ottobre 2010, contiene:

- le finalità e le modalità del trattamento;
- l'indicazione della natura facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- l'ambito di comunicazione e diffusione dei dati;
- i diritti dell'interessato;
- l'indicazione del titolare e del responsabile del trattamento.

L'Azienda, stando la molteplicità delle attività effettuate ed essendo contemplata la possibilità di semplificare l'erogazione dell'informativa e l'acquisizione del consenso limitatamente alle sole attività direttamente finalizzate alla prevenzione, diagnosi, cura e riabilitazione, si avvale della facoltà di acquisizione del consenso al trattamento per i propri utenti *"una tantum"* demandando tale attività agli sportelli PASS-CUP.

I Dirigenti Responsabili del Servizio PASS-CUP devono vigilare sulla regolare acquisizione del consenso da parte degli operatori agli sportelli e sulla corretta raccolta e custodia dei modelli di consenso.

L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di:

- emergenza sanitaria o di igiene pubblica;
- impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, 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 dell'interessato;
- nel caso in cui la prestazione medica può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia

In particolari situazioni, l'informativa può essere resa oralmente e, sempreché possibile, attestata per iscritto.

10.1 - *Informative specifiche utenti*

Per particolari casi di trattamento di dati o prestazioni che presuppongono maggiori crucialità di trattamento di dati (quali: servizi per tossicodipendenze, salute mentale, interruzioni volontarie della gravidanza, attività di trapianto, procreazione medicalmente assistita e simili), il *Responsabile* del trattamento della Struttura (Ser.T., DSM, Reparto ospedaliero, ecc.) deve erogare un'ulteriore e specifica informativa ed acquisire un ulteriore e specifico consenso che verrà custodito presso la medesima struttura.

I Responsabili devono utilizzare normalmente i modelli di informativa e/o consenso allegati al Provvedimento n. 1251 del 27 ottobre 2010 con cui sono stati approvati i modelli da utilizzare nelle procedure connesse alla tutela della privacy.

Al personale dipendente, al personale medico convenzionato, ai soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, agli specializzandi, ai tirocinanti, agli allievi ed ai docenti di corsi, ai volontari, agli operatori del servizio civile, ecc., in sede d'instaurazione dei relativi rapporti (nel contratto di lavoro per i dipendenti, nella lettera di incarico per i medici convenzionati e per i docenti, nel modulo di iscrizione per gli allievi, nel contratto libero-professionale per i consulenti ed i liberi professionisti, nella lettera di autorizzazione per i tirocinanti, gli specializzandi ed i volontari, ecc.). le Strutture competenti devono fornire la specifica informativa approvata con il provvedimento del D.G. 1251/2010.

A tutti i contraenti (anche a titolo non oneroso, come le ONLUS), la struttura competente deve erogare l'informativa di rito approvata con il provvedimento del D.G. 1251/2010; tale procedura va

replicata ogni qualvolta si modifichino norme rilevanti che incidono in maniera sostanziale sui contenuti dell'informativa.

Alle Ditte partecipanti a gare di forniture di beni e/o servizi di affidamento dei lavori, ai candidati di concorsi o di avvisi pubblici, l'informativa viene resa in sede di pubblicazione dei relativi bandi con l'indicazione del *Responsabile del trattamento* dei dati relativi alle suindicate procedure.

In tutte le altre ipotesi di trattamento dati, l'Azienda deve utilizzare una formula di informativa analoga alla seguente ed eventualmente adattata alla fattispecie particolare: "*Il trattamento dei dati personali, anche di natura sensibile o giudiziaria, forniti in relazione alla presente procedura è finalizzato unicamente per la gestione della stessa. Il trattamento sarà effettuato dai soggetti incaricati, con l'utilizzo di procedure anche informatizzate, in grado di tutelare e garantire la riservatezza dei dati, secondo quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196*".

ARTICOLO 11 - Trattamento dei dati del personale dipendente e assimilato

L'Azienda tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, così come specificato dall'art. 112 del Codice. Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso dei requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, di adempiere a specifici obblighi in materia di igiene e sicurezza del lavoro, di accertare la responsabilità civile, disciplinare e contabile dei dipendenti. Per il trattamento dei dati del personale dipendente non è necessario richiedere il consenso dell'interessato. La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando, piuttosto, diciture generiche o codici numerici.

All'atto del reclutamento di personale (sanitario, amm.vo, ecc.) con rapporto di lavoro dipendente (prima assunzione o proroga) o a qualsiasi altro titolo, i Responsabili amm.vi delle UU.OO. competenti devono inserire nel contratto/convenzione una specifica clausola (ALL.6) che preveda, in ossequio a quanto disposto dal D.G. con i provvedimenti di approvazione "ambiti di trattamento consentiti", la formale designazione ad "*incaricato*".

ARTICOLO 12 - Trattamento dei dati sanitari

L'Azienda, in quanto organismo sanitario pubblico, può trattare i dati personali idonei a rivelare lo stato di salute *con il consenso dell'interessato e sulla base dell'autorizzazione del Garante*, in conformità alle disposizioni dettate nel D. Lgs. 196/03, e, in particolare, nella Parte II, Titolo V.
I due requisiti indicati possono essere richiesti alternativamente nelle seguenti ipotesi:

- 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;
- 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.

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. Negli articoli che seguono si riportano, tra le altre, le tutele da rispettare relativamente alla comunicabilità dei dati dei ricoverati, al ritiro delle refertazioni e alle informazioni che gli operatori sanitari possono fornire a seguito di richieste di terzi.

12.1 - ***Manifestazione volontà ricoverati***

Il paziente ricoverato può indicare, avvalendosi della modulistica aziendale:

- se si può o meno comunicare a terzi la circostanza del ricovero;
- i soggetti ai quali possono essere comunicate le informazioni relative al proprio stato di salute.

Gli operatori sanitari sono tenuti, nell'adempimento delle loro mansioni, ad assicurarsi che venga sempre utilizzata la modulistica aziendale per la comunicabilità della volontà del ricoverato, da inserire nella cartella clinica in modo che il personale sanitario sia in grado, in ogni momento di verificare l'indicazione dei soggetti ai quali possono essere rilasciate informazioni sullo stato di salute del paziente. Il Responsabile del trattamento interessato deve vigilare in ordine all'adempimento di tale obbligo.

12.2 - ***Delega ritiro refertazioni***

Le refertazioni relative agli esami eseguiti devono essere consegnate:

- al diretto interessato;
- al soggetto che esercita la tutela, in caso di minore o interdetto;

- al soggetto delegato indicato nell'apposito modulo aziendale, munito di delega, documento proprio e documento del delegante;

Gli operatori sanitari preposti al rilascio delle refertazioni, sono tenuti a verificare, in caso di ritiro delle stesse ad opera di persona diversa dal diretto interessato, che venga sempre utilizzata la modulistica aziendale predisposta per la delega. Il *Responsabile del trattamento* interessato deve vigilare in ordine all'adempimento di tale obbligo.

12.3 - ***Modulistica***

L'Azienda ha adottato con provvedimento del D.G. n. 1251/2010 modelli uniformi di informativa (pubblicati sul sito www.asrem.it) ed allegati al presente Regolamento. Eventuali ulteriori modelli da adottare per specifiche esigenze organizzative delle Strutture sono predisposti dai *Responsabili del trattamento*, in relazione alle rispettive competenze, con la collaborazione del *Referente Privacy.*

12.4 - ***Rilascio di informazioni relativamente alle prestazioni di pronto soccorso e alla dislocazione del paziente in un reparto***

Gli operatori sanitari possono dare notizia, anche per via telefonica, ai terzi legittimati (quali possono essere familiari, parenti o conviventi) valutate le diverse circostanze del caso, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica.

Gli operatori sanitari possono altresì fornire informazioni, anche per via telefonica, ai terzi legittimati (quali possono essere familiari, parenti o conviventi) valutate le diverse circostanze del caso, circa la dislocazione dei degenti nei reparti e salvo una diversa volontà dell'interessato manifestata ai sensi dell'art. 11. 1 comma 1.

In nessun caso possono essere rilasciate informazioni generiche o circostanziate sullo stato di salute.

12.5 - ***Procedure organizzative a tutela della riservatezza in ambiente sanitari.***

Gli operatori e le strutture sanitarie sono tenuti ad osservare le disposizioni di cui al Provvedimento del Garante per la Protezione dei dati Personali del 9 novembre 2005 recante i precetti da onorare nell'adempimento dei compiti di prevenzione, diagnosi, cura e riabilitazione, nonché le regole richiamate nel Vademecum Garante per la Protezione dei dati Personali 2011.

Presso tutti i presidi dell'Azienda, a cura dei Responsabili delle Strutture, sono adottate procedure, quali l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, etc.) o amministrative (rimborsi, indennità, ecc.). I

responsabili dei trattamenti sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con familiari, ecc.) o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati. Le strutture ospedaliere possono fornire informazioni sui degenti, anche tramite il centralino telefonico, limitatamente alla loro presenza in ospedale e sulla loro collocazione all'interno della struttura, salvo che il degente chieda di non rendere nota la sua presenza. Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

Articolo 13 - Misure di sicurezza dei dati

La normativa sulla privacy considera il trattamento dei dati personali come un'attività particolarmente critica, tanto da assimilarla, dal punto di vista dell'eventuale risarcimento del danno, alle c.d. attività pericolose di cui all'art. 2050 codice civile.
Per questa ragione, la legge detta alcune regole concernenti la sicurezza dei dati, distinguendo le Misure '*minime*' di sicurezza dalle Misure cosiddette "*idonee*".
La violazione delle prime, che concretizza l'illecito di omessa adozione delle Misure minime di sicurezza può comportare l'irrogazione di sanzioni di natura penale e amministrativa. L'Allegato 'B' al Codice Privacy, "Disciplinare tecnico in materia di misure minime di sicurezza", descrive le misure minime obbligatorie, distinguendo i trattamenti effettuati con strumenti elettronici da quelli effettuati senza strumenti elettronici, dosando le misure a seconda che i dati trattati siano comuni oppure sensibili/giudiziari oppure sanitari oppure genetici. Le modifiche introdotte dal D.L. 5/2012 hanno determinato l'abrogazione della misura minima di sicurezza consistente nella redazione del DPS (il Documento programmatico sulla sicurezza) o dell'autocertificazione o, in luogo del DPS, dell'adozione delle altre misure minime. L'abrogazione ha avuto anche l'effetto di eliminare il reato omissivo in cui incorreva il titolare del trattamento elettronico di dati sensibili che non avesse approvato entro il 31 marzo di ciascun anno il DPS (art. 169 Codice Privacy) e, parimenti, è venuta meno la relativa sanzione amministrativa (art. 162, comma II bis).
L'Azienda garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta, anche attraverso la redazione di istruzioni e di opuscoli informativi (*rif. al manuale "Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i. pubblicato sul sito aziendale*).

Il livello minimo di protezione dei dati e dei relativi trattamenti è assicurato dall'adozione delle misure minime di sicurezza, cioè dal complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali aziendali che scaturiscono dalle normative ed indicazioni del Garante in materia.

L'Azienda, periodicamente, promuove iniziative tese a verificare il livello di attuazione delle misure di sicurezza privacy adottate nelle diverse Strutture/Servizi aziendali e vigila sulla puntuale osservanza dei compiti e delle istruzioni impartite ai diversi soggetti competenti in materia di protezione dei dati personali.

Articolo 14 - Diritto di accesso agli atti

Fatti salvi gli atti sottratti all'accesso per norma di legge o di regolamento, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa a chiunque abbia un interesse personale e concreto per la tutela di situazioni giuridicamente rilevanti, ai sensi degli articoli 59 e 60 del Codice, dell'articolo 22 della 18 legge 7 agosto 1990, n. 241, e dell'articolo 2 del D.P.R. 27 giugno 1992, n. 352, nonché nell'esercizio dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. Nel caso l'istanza di accesso riguardi documentazione contenente dati riservati, comuni o sensibili, di terzi, salvo quanto previsto al comma 3, l'accesso è limitato alla sola visione dei dati la cui conoscenza sia necessaria per curare o difendere un proprio interesse giuridico, nel rispetto dei principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso stesso. Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito a condizione che ciò si renda necessario per far valere o difendere in sede giudiziaria una situazione giuridicamente rilevante di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso stesso.

E' comunque garantito l'accesso agli atti amministrativi che non contengono dati personali di soggetti diversi da quelli del richiedente, sempreché ricorrano i presupposti previsti dall'articolo 22 della legge 7 agosto 1990, n. 241, e dall'articolo 2 del D.P.R. 27 giugno 1992, n. 352.

Il *responsabile* dell'U.O. che, per le funzioni di sua competenza, è in possesso dell'informazione, ha formato l'atto o il provvedimento o lo detiene stabilmente, è tenuto ad evadere le richieste di accesso conformemente a quanto previsto dal Regolamento per l'accesso agli atti ed alle informazioni, nel rispetto della tutela dei dati personali adottato con provvedimento del D.G. n. 1480 del 20/11/2009.

Qualora la predetta richiesta coinvolga l'applicazione della disciplina in materia di protezione dei dati personali, è possibile richiedere un parere al Referente privacy.

Per i diritti dell'interessato in ordine all'accesso e al trattamento dei propri dati personali si applicano le disposizioni previste dagli art. 8-9-10 del Codice.

I *Responsabili* del Trattamento sono tenuti al riscontro delle richieste degli interessati. L'interessato può inoltrare la richiesta, formulata ai sensi dell'art. 7 del D. Lgs. 196/03:

- direttamente al *Responsabile* del Trattamento che conserva e gestisce i suoi dati;
- all'Ufficio Protocollo Generale dell'Azienda, che ne curerà l'inoltro al competente *Responsabile* del Trattamento.

Alle richieste degli interessati deve essere fornito riscontro tempestivamente ai sensi dell'art. 8 del D. Lgs. 196/03.

14.1 - *Cartelle cliniche*

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

- di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- in caso di decesso dell'interessato, per esigenze di tutela dello stesso o per ragioni familiari meritevoli di protezione (prendendo come punto di riferimento, in questa ultima ipotesi, il grado di parentela - che deve essere autocertificato dal richiedente - secondo l'ordine previsto nella successione legittima ex artt. 565 e segg. del Codice Civile).

Nella valutazione del "*pari rango*" che può giustificare l'accesso è necessario utilizzare come parametro di raffronto non il diritto di azione e difesa di per sé, ma il diritto sottostante che il terzo intende far valere sulla base del materiale documentale che chiede di conoscere.

Occorre, inoltre, tenere presente che deve essere negato l'accesso:

- se è volto a soddisfare generiche esigenze basate sulla prospettiva eventuale di apprestare la difesa di diritti non posti in discussione in quel momento;
- nella maggior parte dei casi riguardanti diritti di credito.

Va valutata con cautela, caso per caso, l'effettiva necessità di consentire l'accesso ad una cartella clinica in caso di controversia per risarcimento dei danni ascritti all'attività professionale medica

documentata nella cartella. Deve essere sempre esibita la cartella su disposizione dell'autorità giudiziaria o di polizia. Nel caso in cui l'Azienda ritenga di dover accogliere l'istanza di accesso, deve essere effettuata una valutazione concreta, particolarmente accurata, su quali informazioni, fra quelle contenute nei documenti oggetto della richiesta, debbano essere comunicate e quali siano, invece, eccedenti rispetto allo scopo perseguito con l'accesso.

14.2 ***- Indagini difensive***

Nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art.391-quater del Codice di Procedura Penale, ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito

Ai fini di tali indagini, il difensore può chiedere documenti in possesso dell'Azienda (e può estrarne copia a proprie spese) anche se contengono dati personali di un terzo interessato e senza la necessità del suo consenso. Se nei documenti richiesti sono contenuti dati idonei a rivelare lo stato di salute o la vita sessuale, il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile

Articolo 15 - La pubblicazione degli atti

L'Azienda osserva le disposizioni di cui alla Legge n. 69 del 18 giugno 2009 recante la disciplina da osservare in materia di pubblicazione on line di atti e provvedimenti della Pubblica Amministrazione, le disposizioni di cui al Codice Privacy e i provvedimenti del Garante privacy dettati in materia, in particolare quello che detta le "Linee guida in materia di trattamento dei dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" pubblicato sulla G.U. del 19 marzo 2011.

L'Azienda nella pubblicazione degli atti on line, può trattare i dati personali, diversi da quelli sensibili e giudiziari, anche in assenza di norme di legge o di regolamento e senza il consenso dell'interessato, nel caso in cui il trattamento sia necessario per adempiere a compiti istituzionali. Qualora le operazioni di trattamento coinvolgano i dati sensibili e giudiziari, le stesse sono consentite soltanto se autorizzate da espressa disposizione di legge nella quale siano specificati le tipologie di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite, ovvero qualora tale operazioni siano identificate nel cd. "Regolamento privacy", di cui all'art. 20 del D. Lgs. 196/03. Per l'Azienda tale atto è stato adottato con Regolamento Regionale 23 ottobre 2006 n. 4 (Trattamento di dati sensibili e giudiziari) pubblicato sull BURM del 24 ottobre 2006

15.1 - ***Divieto di diffusione***

Il rispetto delle disposizioni di cui alla L. n. 69 del 18 giugno 2009 non comporta deroga al generale divieto di diffusione dei dati idonei a rivelare lo stato di salute, così come il rispetto, ad opera delle Amministrazioni pubbliche, dei principi di necessità e proporzionalità di cui agli artt. 3 ed 11 del Codice .

15.2 - ***Cautele tecniche***

La pubblicazione degli atti on line deve essere assistita da misure e accorgimenti tecnici volti a garantire un accesso calibrato agli atti e ai documenti, ovvero diverso a seconda che la stessa avvenga per finalità di trasparenza, pubblicità o consultabilità, onde evitare una promiscua disponibilità degli stessi.
I dati pubblicati on line non devono essere incondizionatamente reperibili in rete, ad esempio mediante motori di ricerca esterni al sito e la loro permanenza on line deve avere una durata congrua, fermo restando il rispetto del lasso di tempo eventualmente già individuato dalla legge. Occorre altresì adottare soluzioni tecniche volte ad evitare la duplicazione massiva dei file e la decontestualizzazione dei dati.
In definitiva, il rispetto dei principi e delle disposizioni in materia di riservatezza dei dati personali, anche in relazione alla pubblicazione obbligatoria all'Albo Pretorio Informatico, va assicurato con idonee misure o accorgimenti tecnici da attuare in sede di redazione dell'atto stesso da parte del soggetto competente.
Il soggetto, l'ufficio o l'organo che propone e/o adotta l'atto da pubblicare è responsabile del contenuto degli atti pubblicati in relazione al rispetto delle norme sulla protezione dei dati personali e quindi, anche per gli aspetti correlati alla loro diffusione tramite l'Albo Pretorio Informatico.

15.3 - ***Provvedimenti aziendali***

Le regole da osservare nella redazione e pubblicazione degli atti sono inserite nel provvedimento del D.G. n. 1685/2010 disponibile sul sito web aziendale e nel Documento di analisi redatto dalla struttura Privacy, contenente le cautele da adottare per elevare la qualità "privacy" degli atti prodotti dai Responsabili delle UU.OO. amministrative.

Articolo 16 - Responsabilità in caso di violazione delle disposizioni sulla privacy

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale nelle ipotesi previste dagli articoli da 161 a 172

del Codice. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del Codice Civile (responsabilità per esercizio di attività pericolosa). In tale ipotesi vi è una presunzione di responsabilità che può essere superata solo con la dimostrazione di aver adottato tutte le misure idonee ad evitare il danno.

Articolo 17 - Norma finale

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni ed integrazioni).

Riferimenti normativi, provvedimenti ed atti di indirizzo

1. Decreto Legislativo n. 196/2003 (Codice in materia di Protezione dei Dati Personali)
2. Decreto Legislativo n. 5/2012 (Codice in materia di Protezione dei Dati Personali) cosiddetto *"decreto semplificazione"*
3. Legge n. 69 del 18 giugno 2009:" Disciplina da osservare in materia di pubblicazione on line di atti e provvedimenti della Pubblica Amministrazione"
4. Provvedimento Generale del Garante del 09/11/2005:
5. Provvedimento Generale del Garante del 27/11/2008: "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema"
6. Provvedimento generale del Garante dell'8 aprile 2010 "Provvedimento in materia di videosorveglianza - 8 aprile 2010
7. Vademecum per la Protezione dei dati Personali 2011 redatto dal Garante
8. Linee guida del Garante in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" - Gazzetta Ufficiale del 19 marzo 2011
9. Provvedimento generale del Garante del 15 maggio 2014 "Linee guida in materia di trattamento dei dati personali contenuti anche in atti e documenti amministrativi, effettuati con finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"
10. Delibera del Consiglio Regionale n. 192/2006: Regolamento n. 4 del 23 ottobre 2006 "Regolamento per il trattamento di dati sensibili e giudiziari"
11. Provvedimento del Direttore Generale. N 305 del 09.05.2007
12. Provvedimento del Direttore Generale. n. 628/2007"Adozione del regolamento interno per lo scarto del materiale cartaceo"
13. Provvedimento del Direttore Generale n. 360 del 17 aprile 2008 "Approvazione di schemi-tipo relativi a protocolli d'intesa operativi inerenti la gestione e lo scambio di dati personali per la realizzazione di finalità istituzionali"
14. Provvedimento del Direttore Generale n. 927 del 12.08.2010 "Modello organizzativo ed individuazione dei soggetti competenti in materia di protezione dei dati personali"
15. Provvedimento del Direttore Generale n. 1052 del 29.07.2011 "Integrazione Provvedimento n. 927 del 12.08.2010 - Modello organizzativo ed individuazione dei soggetti competenti in materia di protezione dei dati persona"
16. Provvedimento del Direttore Generale n.1686/ 2010 "Affidamento incarico di Referente Aziendale del servizio informatico Asrem e attribuzione funzione di Amministratore di sistema interno"
17. Provvedimento del Direttore Generale n. 1627/2009 :"Regolamento Aziendale per l'utilizzo delle postazioni di informatica individuale, di utilizzo della posta elettronica e della rete Internet aziendale

18. Manuale: “Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i.,”
19. Provvedimento del Direttore Generale n. 1251 del 27 ottobre 2010:” Codice in materia di protezione dei dati personali: approvazione modulistica”
20. Provvedimento del Direttore Generale n.1252 del 27/10 /2010: “Ambiti di trattamento consentiti al personale ospedaliero”
21. provvedimento del Direttore Generale n. 285 del 01/03/2011” Ambiti di trattamento Area Amm.va e Tecnica”
22. Provvedimento del Direttore Generale n. 286 del 01/03/2011” Ambiti di trattamento Direzione sanitaria Presidi Ospedalieri”
23. Provvedimento del Direttore Generale n. 287 del 01/03/2011” Ambiti di trattamento Direzione amministrativa dei Presidi Ospedalieri”
24. Provvedimento del Direttore Generale n. 288 del 01/03/2011” Ambiti di trattamento Dipartimento di Emergenza e 118”
25. Provvedimento del Direttore Generale n. 289 del 01/03/2011” Ambiti di trattamento Area Sovradistrettuale”
26. Provvedimento del Direttore Generale n. 290 del 01/03/2011” Ambiti di trattamento Dipartimento di Salute Mentale”
27. provvedimento del Direttore Generale n. 412 del 30/03/2011” Ambiti di trattamento Dipartimento di Prevenzione”
28. provvedimento del Direttore Generale n. 580 del 27/04/2011” Ambiti di trattamento Area Distrettuale”
29. provvedimento del Direttore Generale n. 29 del 10/01/2014 “Ambiti di trattamento consentiti al personale dell’area distrettuale” - integrazione
30. provvedimento del Direttore Generale n.1480 del 20/11/2009 “Regolamento di accesso agli atti ed alle informazioni nel rispetto della tutela dei dati personali”
31. provvedimento del Direttore Generale n. 1685/2010: “Approvazione documento linee guida pubblicazione atti”
32. nota di indirizzo della struttura Privacy avente ad oggetto “indirizzi operativi privacy nell’ambito delle procedure di affidamento di acquisizione di beni e servizi” data 30/07/2010 prot. 57 PY
33. nota di indirizzo della struttura Privacy avente ad oggetto: “assunzione personale ospedaliero: clausola contrattuale” data 15/11/2010 prot. 141 PY
34. nota di indirizzo della struttura Privacy avente ad oggetto: “comunicazione individuazione ambiti di trattamento” data 09/03/2011 prot. 3378
35. nota di indirizzo della struttura Privacy avente ad oggetto: “proroga contratti di collaborazione coordinata e continuativa - clausola contrattuale” data 13/07/2011 prot. n.10783
36. documento di analisi redatto dalla struttura Privacy avente ad oggetto:”tutele privacy nella pubblicazione dei provvedimenti sull’Albo Pretorio on-line” - data 2/08/2011 prot .n. 11710

Sommario

Articolo 1 - Oggetto e finalità 1
1.1- ***Norme di rinvio*** 1
Articolo 2 - Organigramma privacy 1
2.1 - ***Titolare del trattamento*** 2
2.2 - ***Responsabili del trattamento*** 2
2.3 - ***Responsabili interni*** 4
2.4 - ***Responsabili esterni*** 4
2.5 - ***Incaricati del trattamento interni*** 6
2.6 - ***Incaricati esterni del trattamento che operano all'interno dell'azienda*** 7
2.7 - ***Referente aziendale per la Privacy*** 7
2.8 - ***Amministratori di sistema*** 8
2.9 - ***Diritti dell'interessato*** 9
Articolo 3 - Il trattamento dei dati 10
Articolo 4 - Principi fondamentali del trattamento dei dati 11
Articolo 5 - Conservazione e sicurezza dei dati 11
Articolo 6 - Censimento dei Trattamenti dei Dati 12
Articolo 7 - Modalità di trattamento dei dati 13
7.1 - ***Trattamento dei dati senza l'ausilio di macchine e strumenti elettronici*** 13
7.2 - ***Trattamento dei dati con l'ausilio di macchine e strumenti elettronici*** 14
Art. 8 - Il trattamento dei dati personali ordinari 14
Articolo 9 - Il trattamento dei dati sensibili e giudiziari 15
9.1 - ***Comunicazione e diffusione*** 15
9.2 - ***Comunicazione di dati all'interessato relativi allo stato di salute*** 15
ARTICOLO 10 - Informativa e Consenso 16
10.1 - ***Informative specifiche utenti*** 17
ARTICOLO 11 - Trattamento dei dati del personale dipendente e assimilato 18
ARTICOLO 12 - Trattamento dei dati sanitari 19
12.1 - ***Manifestazione volontà ricoverati*** 19
12.2 - ***Delega ritiro refertazioni*** 19
12.3 - ***Modulistica*** 20
12.4 - ***Rilascio di informazioni relativamente alle prestazioni di pronto soccorso e alla dislocazione del paziente in un reparto*** 20
12.5 - ***Procedure organizzative a tutela della riservatezza in ambiente sanitari.*** 20
Articolo 13 - Misure di sicurezza dei dati 21
Articolo 14 - Diritto di accesso agli atti 22
14.1 - ***Cartelle cliniche*** 23
14.2 - ***Indagini difensive*** 24
Articolo 15 - La pubblicazione degli atti 24
15.1 - ***Divieto di diffusione*** 25
15.2 - ***Cautele tecniche*** 25
15.3 - ***Provvedimenti aziendali*** 25
Articolo 16 - Responsabilità in caso di violazione delle disposizioni sulla privacy 25
Articolo 17 - Norma finale 26

ALLEGATO 1 – Modello di nomina di 'Responsabile interno' del trattamento

Al dott. _____

Oggetto: Nomina di responsabile di trattamento dati personali (art. 29 D.Lgs. n. 196/2003).

In esecuzione del Provvedimento D.G. n. 927/2010 integrato con successivo Provvedimento D.G. n. 1052/2011, l'Azienda Sanitaria Regionale del Molise, in qualità di Titolare del trattamento dei dati personali, considerato che la S.V. possiede le competenze richieste, in termini di esperienza, capacità, affidabilità per garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza (art. 29, comma 2 del D.Lgs. 196/03), Le conferisce la nomina di Responsabile del Trattamento dei dati personali effettuati nell'ambito della U.O. da lei diretta, affidandole i compiti che la legge pone a carico di questa figura per l'effettuazione, nel rispetto delle prescrizioni della legge e delle modalità precisate nella presente, delle operazioni di trattamento di dati personali relativi a tale funzione.

La S.V. - in ossequio a quanto disposto dalla normativa vigente - procederà a tutte le operazioni di trattamento informatico e/o manuale dei menzionati dati personali, previste dalle citate norme legislative e necessarie per l'espletamento dei compiti attinenti alla Sua funzione, nel rispetto della specifica disciplina in materia di protezione dei dati personali.

Nell'adempimento delle mansioni affidate, la S.V. in particolare dovrà:

a) operare in modo che siano ridotti al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
b) designare i soggetti 'incaricati', definendone livelli di autorizzazione all'accesso ai dati e modalità di esecuzione delle attività demandate e formalizzandone ruolo e responsabilità ai sensi della disciplina vigente; la designazione degli incaricati va effettuata nei servizi relativamente ai quali l'Azienda non vi abbia provveduto tramite preventiva individuazione degli ambiti di trattamento consentiti;
c) curare che ai soggetti interessati (ovvero a coloro i cui dati vengono trattati nell'ambito della funzione di Responsabile dei Trattamenti) venga erogata l'Informativa prevista secondo i modelli forniti dall'Azienda e che da parte degli stessi venga acquisito il consenso al trattamento nei casi previsti;
d) avvertire immediatamente il Titolare di ogni richiesta, provvedimento, accertamento, controllo da parte del Garante o dell'Autorità giudiziaria;
e) ottemperare, oltre che alle disposizioni di legge in materia ed ai provvedimenti delle competenti Autorità, alle istruzioni che il Titolare vorrà impartire in ordine alla sua attività di Responsabile ed ai regolamenti e/o provvedimenti adottati a livello aziendale per la protezione dei dati personali.

È opportuno ricordare che la nomina dei responsabili – facoltativa per legge - non esonera il Titolare dalla cura e dalle responsabilità derivanti dalla disciplina sulla Protezione dei Dati Personali, e pertanto i Responsabili, lungi dal 'sostituire' il Titolare, semmai lo 'affiancano', condividendo cura e responsabilità connesse; pertanto in capo ai Responsabili non titolari di budget non grava alcun obbligo di procurarsi strumenti e risorse di cui non dispongono, mentre essi sono piuttosto tenuti a far rispettare 'per quanto possibile' le norme esistenti o appositamente emanate, segnalando anzi al Titolare situazioni di rischio specifico o fabbisogno di risorse strutturali aggiuntive. Questo tuttavia non esime i Responsabili dall'obbligo dall'attivazione di tutte quelle azioni cruciali relativamente alle quali non vi sono ostacoli di sorta.

Lì,_____

F.to Il Titolare del Trattamento
(Il Direttore Generale)

Il Responsabile del Trattamento
(timbro e firma leggibile)
_____

ALLEGATO 2 - Atto unilaterale d'obbligo in caso di affidamento di servizi che comportano il trattamento di dati personali

In caso di aggiudicazione, il concorrente si obbliga - senza alcun onere aggiuntivo a carico dell'Ente - ad accettare il ruolo di Responsabile del trattamento dei dati personali così come individuato all'art. 29 del Codice privacy ovvero a sottoscrivere Protocollo d'intesa circa le modalità del trattamento dei dati personali, a discrezione dell'Ente.

ALLEGATO 3 - Modello di nomina 'Responsabile esterno' del trattamento

Spett.le Ditta _____
via _____
_____

Oggetto: *Conferimento incarico di "Responsabile esterno" del trattamento dei dati personali e sensibili ai sensi degli artt. 4 co.1, lett. b),d),g) e 29 del D.Lgs. n. 196/2003*

In esecuzione del Provvedimento D.G. n. 927 del 12.08.2010 l'Azienda Sanitaria Regionale del Molise, in qualità di Titolare del trattamento dei dati personali, considerato che la S.V. possiede le competenze richieste in termini di esperienza, capacità, affidabilità per garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza (art. 29, comma 2 del D.lgs. 196/03), Le conferisce la nomina di Responsabile del Trattamento dei dati personali effettuati nel ruolo di **affidatario del Servizio di _____,** conferendoLe i compiti che la legge pone a carico di questa figura per l'effettuazione, nel rispetto delle prescrizioni della legge e delle modalità precisate nella presente, delle operazioni di trattamento di dati personali relativi a tale funzione.

La S.V. - in ossequio a quanto disposto dalla normativa vigente - procederà a tutte le operazioni di trattamento informatico e/o manuale dei menzionati dati personali previste dalla citate norme legislative e necessarie per l'espletamento dei compiti attinenti alla Sua funzione, nel rispetto della specifica disciplina in materia di protezione dei dati personali; si rammenta, in particolare, che non è consentito comunicare i dati trattati ad alcun soggetto terzo, né pubblico né privato.

Nell'adempimento delle mansioni affidate, la S.V. in particolare dovrà:

a) operare in modo che siano ridotti al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
b) designare i soggetti 'incaricati', definendone livelli di autorizzazione all'accesso ai dati e modalità di esecuzione delle attività demandate e formalizzandone ruolo e responsabilità ai sensi della disciplina vigente; la designazione dovrà comprendere l'esplicita indicazione della sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regola di condotte analoghe al segreto professionale, ovvero obbligo di rispettare il segreto assoluto sui dati di cui verrà a conoscenza, così come espressamente previsto dal Codice Privacy, art. 83 comma 2 lettera i);
c) garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato;
di specificare i luoghi dove fisicamente avviene il trattamento dei dati;
d) trasmettere al Direttore dell'U.O. a cui afferisce il servizio l'elenco nominativo degli incaricati con l'indicazione specifica delle relative mansioni;
e) curare che, nei casi previsti, venga erogata l'informativa ai soggetti 'interessati' e che da parte degli stessi venga acquisito il consenso al trattamento dei dati;
f) avvertire immediatamente il Titolare in caso di situazioni anomale di emergenza e di ogni richiesta, provvedimento, accertamento, controllo da parte del Garante o dell'Autorità giudiziaria qualora l'attività ispettiva si riferisca ad attività di cui la ASREM è Titolare dei trattamenti;
g) ottemperare, oltre che alle disposizioni di legge in materia ed ai provvedimenti delle competenti Autorità, alle istruzioni che il Titolare vorrà impartire in ordine alla sua attività di Responsabile e ai regolamenti e/o provvedimenti adottati a livello aziendale per la protezione dei dati personali; in particolare Codesta Azienda dovrà produrre idonea attestazione sulla conformità delle risorse utilizzate (sia fisiche sia informatiche) alla normativa rilevante in materia, con particolare riferimento all'adozione delle misure minime di sicurezza di cui agli artt. 34 e 35 del Codice privacy nonché all'allegato B.
h) relazionare annualmente sulle misure di sicurezza adottate;
i) _____;
l) _____.

Ai sensi e per gli effetti dell'art. 29 co 5, il Titolare del trattamento vigila, anche tramite verifiche periodiche, sulla puntuale osservanza dei compiti e delle istruzioni impartite.

La presente nomina è condizionata per oggetto e durata al contratto in corso di esecuzione tra l'Azienda Sanitaria del Molise e la Ditta e si intenderà revocata di diritto alla cessazione del rapporto medesimo o alla risoluzione per qualsiasi causa dello stesso.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

La presente viene consegnata alla S.V. in duplice copia con preghiera di restituirne un esemplare espressamente datato e sottoscritto.

Lì _____

Per accettazione

Il Titolare del Trattamento
Il Direttore Generale A.S.Re.M.

Il Responsabile del Trattamento

_____

_____
(timbro e firma leggibile del Rappresentante legale o della persona incaricata)

NB: ai punti i, l, vanno inserite eventuali prescrizioni specifiche in riferimento all'attività esternalizzata

ALLEGATO 4 - Protocollo d'intesa

SCHEMA DI PROTOCOLLO D'INTESA TRA AZIENDA SANITARIA REGIONALE MOLISE E SOCIETÀ / ASSOCIAZIONE / DITTA _____ RELATIVO AL TRATTAMENTO DI DATI PERSONALI IN RELAZIONE ALL'ATTIVITÀ DI _____.

L'Azienda Sanitaria Regionale del Molise con sede in Via Petrella,1 Campobasso, Codice Fiscale e Partita Iva _____, rappresentata dal Direttore Generale _____, d'ora in poi denominata 'Ente';

e

la Società/Associazione/Ditta _____ con sede in ..... Codice Fiscale ..... partita IVA ..... rappresentato da ..... d'ora in poi denominata 'Impresa'/'Associazione';

premesso:

- che l'Impresa/Associazione gestisce per conto dell'Ente (o svolge a Titolo di volontariato) attività di _____, in relazione all'attuazione delle proprie finalità istituzionali, attività di _____;

- che tale attività comporta il trattamento di dati personali tra i soggetti;

- che, pertanto, risulta necessario definire una serie di elementi d'intesa tra l'Impresa e l'ENTE, in relazione alla specificazione delle modalità di trattamento dei dati personali in questione;

convengono, in termini d'intesa, quanto segue

Art. 1 - Oggetto e finalità del protocollo

Il presente Protocollo d'Intesa ha per oggetto la definizione delle modalità di scambio, comunicazione e più in generale di trattamento di dati personali inerenti l'attività di _____.

Art. 2 - Correlazione delle finalità del progetto alle finalità istituzionali degli ENTI

L'attività condotta dall'Impresa/Associazione ha come finalità il miglioramento della qualità dei servizi erogati all'utenza, ed è pertanto strettamente correlata alla realizzazione delle finalità istituzionali dell'Ente in materia di sanità.

Art. 3 - Individuazione delle Banche-Dati nelle quali sono contenuti i dati gestiti in relazione all'attività

I dati personali che l'Impresa/Associazione raccoglie autonomamente o che vengono conferiti dall'Ente o che incidentalmente possono venire a conoscenza dell'Impresa/Associazione sono acquisiti e custoditi in apposite banche-dati cartacee/informatizzate, collocate presso _____, per l'accesso alla quale sono state determinate, a cura dell'Impresa, modalità conformi a quanto previsto dalgli artt. 31 e succ. e allegato B del Codice;

Art. 4- Individuazione del Titolare e del Responsabile dei trattamenti di dati personali gestiti per l'attività eseguita dall'Impresa/Associazione

L'Impresa / Associazione informa l'Ente degli elementi essenziali per l'individuazione della proprio struttura di presidio ai fini Privacy; in particolare comunica all'Ente i nominativi dei responsabili dei trattamenti cui è possibile fare riferimento in relazione all'applicazione delle disposizioni di garanzia ed operative del Codice Privacy in ordine alla gestione, allo scambio ed alla comunicazione dei dati personali inerenti l'attività.
L'Impresa si impegna a fornire all'Ente l'elenco degli addetti espressamente nominati incaricati dei trattamenti (ai sensi dell'art. 30 del D.Lgs. 196/2003) con i relativi profili di autorizzazione ai trattamenti stessi; l'Ente ha la facoltà di controllare in qualsiasi momento che i dati vengono trattati esclusivamente da addetti formalmente incaricati dei trattamenti.

Art. 5 - Modalità specifiche di gestione, trattamento, comunicazione, scambio dei dati tra ENTE ed Impresa/Associazione.

Art. 5.1- Impegni ed obblighi dell'Ente

L'Ente conferisce all'Impresa/Associazione i dati personali relativi agli utenti nel rispetto dei seguenti criteri operativi:

- Il trattamento dei dati è limitato ai dati strettamente indispensabili allo svolgimento dell'attività effettuata, rientrante tra le finalità istituzionali dell'Ente;
- i dati resi accessibili all'Impresa/Associazione sono resi disponibili in forma non eccedente rispetto all'utilizzo che di essi deve essere fatto.

Art. 5.2 - Impegni ed obblighi dell'Impresa

L'Impresa si impegna a rendere conoscibile l'attività effettuata:

a) per la valutazione e l'analisi da parte dei competenti operatori degli Enti – per le parti di specifica competenza;

b) per fini statistici, ma in tal caso i dati saranno resi in forma anonima ed aggregata.

Dei dati forniti dall'ENTE all'Impresa/Associazione o da questa direttamente acquisiti per conto dell'ENTI non potranno essere fatte copie.

L'Impresa/Associazione adotta le misure organizzative e procedurali, sia a rilevanza interna che esterna, necessarie a garantire la sicurezza delle transazioni e delle archiviazioni dei dati stessi.

E' fatto assoluto divieto all'Impresa diffondere i dati personali gestiti in relazione all'attività.

Per il trattamento dei dati personali sensibili inerenti gli utenti l'Impresa è tenuta a dimostrare agli Enti che ogni operazione di trattamento dei dati rientra nell'ambito di quelle consentite dalle Autorizzazioni generali del Garante per la Protezione dei Dati personali.

L'Impresa si impegna inoltre a provvedere, ai sensi dell'art. 37 del Codice, alla notificazione dei dati personali, se dovuto.

Art. 5.3 - Impegni dei sottoscrittori per la corretta gestione dei dati sensibili.

L'Ente e l'Impresa/Associazione procedono al trasferimento ed allo scambio dei dati sensibili solamente se questi sono strettamente indispensabili per lo svolgimento del progetto.
In tal senso:

a) l'Ente è tenuto ad adottare le misure di garanzia previste dall'allegato B ed a mettere l'Impresa/Associazione in condizione di operare efficacemente rispetto a dati cifrati, criptati o resi anonimi;

b) L'Impresa è tenuta ad adottare adeguate misure minime di sicurezza ed a gestire i dati sanitari conformemente agli standard prescelti dagli Enti per la cifratura o la criptazione dei dati stessi.

Art. 6 - Clausola di rinvio

Per quanto non espressamente previsto, in termini di garanzia dei dati personali, nel presente Protocollo d'Intesa si rinvia al D.Lgs. 196/03 (Codice Privacy) ed alle sue successive modificazioni ed integrazioni.

Art. 7 - Controversie
In relazione alle controversie inerenti il presente Protocollo d'Intesa, è competente il Foro di CAMPOBASSO.

Art. 8 - Spese relative al protocollo
Ogni spesa inerente la formalizzazione del presente Protocollo d'Intesa è a carico del/della_____ .

Letto, approvato e sottoscritto.
Campobasso, lì.....

Per l'ASReM Per l'Impresa / Associazione

ALLEGATO 5 - Clausola specifica "Amministratore di sistema esterno"

In caso di affidamento di servizi informatici che ricomprendano l'amministrazione dei sistemi

Come prefigurato dal Provvedimento Generale del Garante per la protezione dei dati personali datato 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i., il concorrente si obbliga - senza alcun onere aggiuntivo a carico dell'Ente - ad assumerne le funzioni, facendo conoscere all'Ente l'elenco dei nominativi preposti alle specifiche funzioni.

ALLEGATO 6 - Clausola specifica per individuazione "dipendenti e personale assimilato" ad incaricato del trattamento

Con riferimento al D.Lgs. 196/2003 "Normativa Privacy" si dà atto che l'U.O. di destinazione è tra quelle per le quali l'ambito di trattamento consentito è stato preventivamente individuato con provvedimenti del D.G. pubblicati sul sito aziendale al link Privacy; pertanto, in ossequio a quanto disposto dall'art. 30 comma 2 del D.Lgs. 196/2003, con la sottoscrizione del presente contratto ed assegnazione a specifica unità, il dipendente/ tirocinante/… è incaricato del trattamento dei dati personali riportato nell'ambito corrispondente al profilo professionale e al Servizio di assegnazione di cui allo specifico documento "*Ambiti di trattamento consentiti*".