

**Azienda Sanitaria
Regionale Molise**



ASREM

REGOLAMENTO AZIENDALE SULLA PRIVACY

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".

La normativa contenuta nel presente Regolamento è diretta 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).

Il Provvedimento n. 927/2010 contiene in allegato il modello di nomina a Responsabile, con l'indicazione delle istruzioni previste dall'art. 29 del Codice.

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 personali 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) 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.

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.

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. La 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, il quale dovrà provvedere a nominare eventuali incaricati.

I Responsabili direttamente o avvalendosi dei soggetti di cui al punto 2.3, sono tenuti a:

- a) applicare la normativa contenuta nel Codice, le disposizioni del Garante, le disposizioni contenute nei provvedimenti del D.G. e nel presente Regolamento, nonché la 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.
- b) osservare le istruzioni impartite dal Titolare nell'atto di nomina ed osservare e far osservare le misure precauzionali individuate nel DPS approvato dall'Azienda;
- c) collaborare con il Referente Privacy provvedendo a:
 - fornire al Referente le informazioni richieste;
 - comunicare tempestivamente al Referente 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.

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 di norma nominati *Responsabili 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.

Pertanto, è opportuno che i Responsabili delle Strutture/Servizi che attivano procedure negoziate, prevedano negli atti di gara (capitolati, lettere di invito, ecc.) l’obbligo del concorrente di accettare, in caso di aggiudicazione, – a discrezione dell’Azienda e senza alcun onere aggiuntivo a carico della stessa - il ruolo di *Responsabile 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).

Al momento dell’affidamento del servizio, il relativo contratto da stipulare tra l’Azienda e l’Impresa aggiudicataria, deve prevedere, in una apposita clausola, 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 del trattamento* o del Protocollo d’intesa.

Copia dell’atto di nomina o del Protocollo d’intesa, debitamente controfirmato, dovrà essere trasmesso dal Responsabile della Struttura competente al Referente Privacy.

In sede di prima applicazione del presente Regolamento, i Responsabili delle Strutture aziendali che stipulano convenzioni o contratti dovranno effettuare una ricognizione dei contratti in essere, al fine di verificare l’apposizione della clausola di cui sopra, provvedendo in mancanza a promuovere la necessaria integrazione dei contratti medesimi mediante apposito atto aggiuntivo.

I Responsabili di tali strutture devono fornire informazioni al Referente Privacy sui contratti in essere (prestazioni di servizi, ecc.) per consentire la formalizzazione delle designazioni ai soggetti indicati al punto 4 del provvedimento del Direttore Generale n. 927/2010.

2.5 – Incaricati del trattamento

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.

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 – Referente 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 privacy, 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;
- verifica periodica sull'attività dei Responsabili del Trattamento rispetto alle istruzioni impartite dal Titolare del trattamento, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- controllo e coordinamento dell'attività dell'Amministratore di sistema;
- aggiornamento, con personale all'uopo incaricato, del Documento Programmatico sulla Sicurezza;

Nell'esercizio delle competenze di cui sopra, deve essere garantita al Referente la collaborazione di tutte le articolazioni organizzative dell'Azienda.

2.7 –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 inoltre, coadiuvare il *Referente* ed i *Responsabili del trattamento* anche nell'individuazione ed applicazione delle misure, sia minime che idonee, volte alla protezione dei dati trattati in Azienda, per quanto di sua competenza.

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, 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 e al Referente per la privacy.

In sede di prima applicazione del presente Regolamento, i Responsabili delle strutture affidatarie di prestazioni di servizi in materia informatica devono fornire informazioni al Referente Privacy sui contratti in essere per consentire la formalizzazione delle designazioni ai soggetti individuati *Amministratori di sistemi*.

Articolo 3 - 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 *Responsabili* 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.

3.1 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 contenente dati personali dovrà essere custodita in armadi dotati di serratura, le cui chiavi dovranno 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.

3.2 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.

3.3 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 richiedono un preventivo parere al Referente Privacy.

Articolo 4 - 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 finalizzati alla tutela della salute o dell'incolumità fisica dell'interessato, occorre acquisire il consenso al trattamento dei dati personali.

L'erogazione dell'informativa compete al Responsabile del trattamento specifico; fermo restando i principali contenuti dell'informativa (art. 13 del Codice), di volta in volta è opportuno adattare l'informativa alla finalità perseguita dal trattamento.

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.

4.1 - Utenti.

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 è avvalsa 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.

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), la 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.

4.2 - Dipendenti e assimilati

Al personale dipendente, ai soggetti con i quali vengono instaurati rapporti di collaborazione o liberi professionali, agli specializzandi, ai tirocinanti, agli allievi e docenti di corso, ai volontari, ecc. viene fornita l'informativa di rito in sede di instaurazione dei relativi rapporti.

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

Il Responsabile dell'U.O.C. "Risorse Umane" deve comunicare al *Referente Privacy* 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.

4.3 - Contraenti

A tutti i contraenti (anche a titolo non oneroso, come le ONLUS) va erogata l'informativa di rito allegata al provvedimento del D.G. 1251/2010; tale procedura va replicata ogni qualvolta si modificano 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, i 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.

Articolo 5 - Il trattamento dei dati sensibili e giudiziari

Tutto il personale che presta servizio, a qualsiasi titolo, presso l'Azienda è tenuto a trattare i dati sensibili e giudiziari indispensabili per l'espletamento delle mansioni di competenza con modalità tali da garantire il rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato.

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.

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 operazioni 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, in quanto Ente strumentale della Regione Molise che esercita funzioni di controllo e vigilanza per i suddetti Enti, con Provvedimento del Direttore Generale n. 305 del 09.05.2007, ha recepito la parte del Regolamento approvato con Delibera del Consiglio Regionale n. 192/2006-relativa ai trattamenti ad essa riferibili .

5.1 – 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 citato, 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.

5.2 – 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 6 - Il trattamento dei dati nel settore sanitario

Il trattamento dei dati nel settore sanitario avviene in conformità alle disposizioni dettate nel D. Lgs. 196/03, e, in particolare, nella Parte II, Titolo V.

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.

6.1 – Manifestazione volontà ricoverati

Il paziente ricoverato può indicare, avvalendosi della modulistica aziendale:

1. se si può o meno comunicare a terzi la circostanza del ricovero;
2. 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 (allegata al provvedimento del D.G. n. 1251/2010) 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.

6.2 – Delega ritiro refertazioni

Le refertazioni relative agli esami eseguiti devono essere consegnate al diretto interessato, oppure, al soggetto delegato indicato nell'apposito modulo aziendale.

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 (allegata al provvedimento del D.G. n. 1251/2010) predisposta per la delega. Il Responsabile del trattamento interessato deve vigilare in ordine all'adempimento di tale obbligo.

6.3 – Modulistica

L'Azienda ha adottato con provvedimento del D.G. n. 1251/2010 appositi modelli (allegati al provvedimento e pubblicati sul sito www.asrem.it al link [privacy-urp](#) sezione [privacy](#)). 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*.

6.4 – 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. 6 comma 1

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

6.5 – Procedure organizzative a tutela della riservatezza in ambiente sanitario.

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.

Articolo 7 - 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. Tra le misure minime di sicurezza da adottare obbligatoriamente qualora vi siano dati sensibili o giudiziari trattati con strumenti elettronici, assume particolare rilevanza la redazione annuale del Documento Programmatico sulla Sicurezza dei dati (di seguito indicato DPS).

7.1 – Documento Programmatico sulla Sicurezza

Ai sensi e per gli effetti degli artt. da 33 a 36 del D.Lgs. 196/2003 e dell'All.B del medesimo Codice, l' Azienda aggiorna annualmente il DPS, sulla base delle analisi dei rischi che incombono sui dati trattati dalle varie strutture/Servizi aziendali, delle misure in essere e da adottare per la messa in sicurezza dei dati medesimi.

Il *referente Privacy* trasmette annualmente ai *Responsabili del Trattamento*, dopo l'adozione del DPS prevista dalla legge entro il 31 marzo, un estratto dello stesso, al fine di metterli a conoscenza dello status degli adempimenti privacy e delle eventuali criticità rilevate nelle strutture da loro dirette.

Articolo 8 - Privacy e accesso agli atti

Il diritto di accesso possiede lo stesso rango del diritto alla protezione dei dati personali: nessuno dei due, può prevalere sull'altro così come nessuno dei due può soccombere 'in nome' dell'altro, non a caso ciascuna delle due normative riconosce il limite derivante dall'altro diritto. Ogni qualvolta si è in presenza di una richiesta di accesso agli atti occorre, dunque, procedere ad un

bilanciamento degli interessi coinvolti, al fine di poter dare corretta esecuzione alla stessa.

Il Codice all'art.59, riconosce esplicitamente l'importanza del diritto di accesso definendo di rilevante interesse pubblico perseguito – e pertanto eseguibili – le attività ad esso finalizzate, ancorché comprendenti dati sensibili o giudiziari.

Lo stesso Codice, tuttavia, all'art. 60 stabilisce che quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

L'Azienda ha adottato con provvedimento del DG n.1480 del 20/11/2009 il “Regolamento di accesso agli atti ed alle informazioni nel rispetto della tutela dei dati personali” , disponibile sul sito web aziendale, che va osservato per evadere le richieste di accesso agli atti formulate dagli interessati.

8.1 – Richieste di accesso agli atti

Ciascun responsabile del procedimento è tenuto ad evadere le richieste di accesso di propria competenza. Qualora la predetta richiesta coinvolga l'applicazione della disciplina in materia di protezione dei dati personali è possibile richiedere un parere al *Referente privacy*.

8.2 – Riscontro alle richieste di cui all'art. 7 del D. Lgs.196/03

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:

1. direttamente al Responsabile del Trattamento che conserva e gestisce i suoi dati;
2. 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.

Articolo 9 - 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.

9.1 - 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 .

9.2 - 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.

9.3 - 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 al link [privacy-urp](#) sezione [privacy](#) 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.

Riferimenti normativi, provvedimenti ed atti di indirizzo

1. Decreto Legislativo n. 196/2003 (Codice in materia di Protezione dei Dati Personali)
2. Legge n. 69 del 18 giugno 2009:” Disciplina da osservare in materia di pubblicazione on line di atti e provvedimenti della Pubblica Amministrazione”
3. Provvedimento Generale del Garante del 09/11/2005:
4. 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”
5. Provvedimento generale del Garante dell’8 aprile 2010 “Provvedimento in materia di videosorveglianza - 8 aprile 2010
6. Vademecum per la Protezione dei dati Personali 2011 redatto dal Garante
7. 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
8. Delibera del Consiglio Regionale n. 192/2006: Regolamento n. 4 del 23 ottobre 2006 “Regolamento per il trattamento di dati sensibili e giudiziari”
9. Provvedimento del Direttore Generale. N 305 del 09.05.2007
10. Provvedimento del Direttore Generale. n. 628/2007”Adozione del regolamento interno per lo scarto del materiale cartaceo”
11. 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”
12. Provvedimento del Direttore Generale n. 927 del 12.08.2010 “Modello organizzativo ed individuazione dei soggetti competenti in materia di protezione dei dati personali”
13. 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”
14. Provvedimento del Direttore Generale n.1686/ 2010 “Affidamento incarico di Referente Aziendale del servizio informatico Asrem e attribuzione funzione di Amministratore di sistema interno”
15. 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
16. manuale: “Istruzioni ai Responsabili e agli incaricati del trattamento dei dati personali ai sensi del D.Lgs. 196/1993 e s.m.i.,”
17. Provvedimento del Direttore Generale n. 1251 del 27 ottobre 2010:” Codice in materia di protezione dei dati personali: approvazione modulistica”

18. provvedimento del Direttore Generale n.1252 del 27/10 /2010: “Ambiti di trattamento consentiti al personale ospedaliero”
19. provvedimento del Direttore Generale n. 285 del 01/03/2011” Ambiti di trattamento Area Amm.va e Tecnica”
20. provvedimento del Direttore Generale n. 286 del 01/03/2011” Ambiti di trattamento Direzione sanitaria Presidi Ospedalieri”
21. provvedimento del Direttore Generale n. 287 del 01/03/2011” Ambiti di trattamento Direzione amministrativa dei Presidi Ospedalieri”
22. provvedimento del Direttore Generale n. 288 del 01/03/2011” Ambiti di trattamento Dipartimento di Emergenza e 118”
23. provvedimento del Direttore Generale n. 289 del 01/03/2011” Ambiti di trattamento Area Sovradistrettuale”
24. provvedimento del Direttore Generale n. 290 del 01/03/2011” Ambiti di trattamento Dipartimento di Salute Mentale”
25. provvedimento del Direttore Generale n. 412 del 30/03/2011” Ambiti di trattamento Dipartimento di Prevenzione”
26. provvedimento del Direttore Generale n. 580 del 27/04/2011” Ambiti di trattamento Area Distrettuale”
27. 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”
28. provvedimento del Direttore Generale n. 1685/2010: “Approvazione documento linee guida pubblicazione atti”
29. 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
30. nota di indirizzo della struttura Privacy avente ad oggetto: “assunzione personale ospedaliero: clausola contrattuale” data 15/11/2010 prot. 141 PY
31. nota di indirizzo della struttura Privacy avente ad oggetto: “comunicazione individuazione ambiti di trattamento” data 09/03/2011 prot. 3378
32. 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
33. 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.....	1
2.2 – Responsabili del trattamento.....	2
2.3 – Responsabili interni.....	2
2.4 – Responsabili esterni.....	3
2.5 – Incaricati del trattamento.....	5
2.6 – Referente per la Privacy.....	5
2.7 –Amministratori di sistema.....	6
Articolo 3 - Modalità di trattamento dei dati.....	7
3.1 Trattamento dei dati senza l’ausilio di macchine e strumenti elettronici.....	7
3.2 Trattamento dei dati con l’ausilio di macchine e strumenti elettronici.....	7
3.3 Uso delle apparecchiature di videosorveglianza.....	8
Articolo 4 - Informativa e Consenso.....	8
4.1 - Utenti.....	8
4.2 - Dipendenti e assimilati.....	9
4.3 - Contraenti.....	9
Articolo 5 - Il trattamento dei dati sensibili e giudiziari.....	9
5.1 – Comunicazione e diffusione.....	10
5.2 – Comunicazione di dati all’interessato relativi allo stato di salute.....	10
Articolo 6 - Il trattamento dei dati nel settore sanitario.....	10
6.1 – Manifestazione volontà ricoverati.....	11
6.2 – Delega ritiro refertazioni.....	11
6.3 – Modulistica.....	11
6.4 – Rilascio di informazioni relativamente alle prestazioni di pronto soccorso e alla dislocazione del paziente in un reparto.....	11
6.5 – Procedure organizzative a tutela della riservatezza in ambiente sanitario.....	12
Articolo 7 - Misure di sicurezza dei dati.....	12
7.1 – Documento Programmatico sulla Sicurezza.....	12
Articolo 8 - Privacy e accesso agli atti.....	12
8.1 – Richieste di accesso agli atti.....	13
8.2 – Riscontro alle richieste di cui all’art. 7 del D. Lgs.196/03.....	13
Articolo 9 - La pubblicazione degli atti.....	13
9.1 – Divieto di diffusione.....	14
9.2 – Cautele tecniche.....	14
9.3 – Provvedimenti aziendali.....	14