AZIENDA OSPEDALIERA "G. Rummo"
Via dell'Angelo, 1 –
Tel. 0824/57511 – Fax 0824/312439
82100 BENEVENTO
P.IVA e C.F. 01009760628

UFFICIO PRIVACY

REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Decreto Legislativo 30 giugno 2003 n. 196
"Codice in materia di protezione dei dati personali"

Approvato con deliberazione del Direttore Generale n. 329 del 22/02/2008

INDICE

Art. 1 – Oggetto -
Il presente regolamento disciplina gli interventi diretti alla tutela della privacy in ambito sanitario. Esso si attiene alle disposizioni attuative del D.lgs 196/03 e rappresenta un atto d'indirizzo in materia di protezione dei dati personali eseguiti, dall'Azienda Ospedaliera di rilievo nazionale "G.RUMMO" di Benevento, nel rispetto della dignità e del diritto alla riservatezza delle persone fisiche e giuridiche, le quali esercitano, a diversi livelli di responsabilità e di funzione, un rapporto diretto o indiretto con l'Azienda.
Esse sono gli utenti, il personale dipendente, i fornitori, gli Enti e gli organismi pubblici e privati.
L'Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di perdita dei dati, di accesso non autorizzato al trattamento oppure di trattamento illecito e non conforme alle finalità della raccolta.
L'Azienda adotta, altresì, le misure necessarie per facilitare l'esercizio dei diritti dell'interessato, ai sensi dell'art. 7 del D.lgs. 196/03.

Art. 2 – Dati personali –
Il dato personale (art. 4, comma 1, lett. B) del D.lgs. 196/03) è qualunque informazione relativa a persona fisica , persona giuridica, Ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Il dato sensibile, ai sensi dell'art. 4, comma 1, lett. D), è quel dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Art. 3 – Trattamento dei dati personali –
Con la denominazione "trattamento", ai sensi dell'art. 4, comma 1, lett. A) del D.lgs. 196/03, deve intendersi qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati, acquisiti dall'interessato.
Qualunque trattamento di dati personali, da parte dell'Azienda, è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2 D.lgs. 196/03), al fine di adempiere a compiti ad essa attribuiti da leggi e/o regolamenti.

Art 4 – Criteri per l'esecuzione del trattamento dei dati personali –
Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto del diritto di riservatezza e della dignità dell'interessato.
Oggetto del trattamento devono essere i soli dati personali necessari per lo svolgimento delle attività istituzionali.
I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati

nelle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
E' compito del Referente privacy aziendale e dei Responsabili del trattamento verificare, per delega del Titolare del trattamento, la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza non eccedenza e necessità rispetto alle finalità perseguite per compiti istituzionali.
I dati che, a seguito di verifiche, risultassero eccedenti, non pertinenti o non necessari, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
I trattamenti di dati effettuati attraverso l'accesso in banche dati, facenti capo a Titolari diversi dall'Azienda (interconnessione di banche dati), sono espletati in base ad espressa disposizione di legge o approvata regolamentazione.

In ogni caso devono adottarsi misure tali da garantire che i dati personali, soprattutto quelli sensibili, siano accessibili ai soli incaricati del trattamento e nella misura strettamente necessaria allo svolgimento delle mansioni di ciascuno.

Art. 5 – Comunicazione dei dati -
La comunicazione dei dati personali, da parte dell'Azienda ad altri soggetti pubblici, è ammessa esclusivamente per fini istituzionali e/o, nei casi in cui vi sia il consenso dell'interessato. Tale consenso viene acquisito previa informativa sulle finalità e le modalità di comunicazione dei suddetti (art. 19, comma 2, D.lgs. 196/03). La diffusione dei dati personali è ammessa unicamente per fini istituzionali, quando sia prevista da una norma di legge o da una regolamentazione d'istituto (art. 19, comma 3, D.lgs. 196/03). Idati idonei a rivelare lo stato di salute non possono essere comunicati senza il consenso dell'interessato (art. 22, comma 8, D.lgs. 196/03). Il consenso del trattamento, acquisito anche verbalmente dall'interessato, è subordinato comunque all'obbligo dell'informativa sulle finalità e modalità di trattamento.

Art. 6 – Informativa all'interessato –
L'informativa sulle finalità e le modalità di trattamento dei dati personali deve essere fornita obbligatoriamente all'interessato. Essa può essere fornita mediante modello cartaceo (da accludere alla cartella clinica) o anche in forma verbale; oppure può essere esibita in formato poster, con l'obbligo di affissione nei locali di maggior transito dell'utenza.
L'informativa deve essere fornita obbligatoriamente, a prescindere dalle modalità di acquisizione del consenso. Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del D.lgs. 196/03 e più specificatamente:

- La tipologia di dati trattati;
- Le finalità e le modalità con le quali vengono trattati i dati;
- L'obbligatorietà o meno del conferimento dei dati;
- I diritti dell'interessato;
- gli estremi identificativi del Titolare e/o del Responsabile al trattamento;

L'informativa all'interessato sulle finalità e le modalità di trattamento dei dati, costituisce parte integrante della cartella clinica adottata dall'Azienda.

Art. 7 - Consenso al trattamento dei dati –
L'Azienda ospedaliera "G.RUMMO" tratta i dati idonei a rilevare lo stato di salute, per fini esclusivamente istituzionali, secondo le modalità previste dalla Legge ovvero:

1. senza acquisire preventivamente il consenso dell'interessato, se il trattamento riguarda operazioni indispensabili a garantire l'immediata tutela della salute o dell'incolumità fisica dell'interessato;
2. previo consenso dell'interessato, acquisito in forma scritta o verbale, se il trattamento dei dati è differibile all'atto assistenziale, il quale non ha carattere di urgenza: ad esempio la raccolta dei dati sensibili inerenti al ricovero in day hospital. In entrambe le modalità resta l'obbligo dell'informativa fornita anche verbalmente.

Il modello per l'acquisizione del consenso dei dati personali, da parte dell'interessato, costituisce parte integrante della cartella clinica adottata dall'Azienda.
Nell'ambito di attività istituzionali "amministrative", concernenti il trattamento dei dati personali, per fini legittimi, non è obbligatorio richiedere il consenso scritto dell'interessato, fermo restando il rispetto dell'obbligo dell'informativa.

Art. 8 – Il Titolare del trattamento dei dati personali –
Ai sensi dell'art. 4, comma 1, lett. F) e degli artt. 28 e 29 del D.lgs. 196/03, l'Azienda ospedaliera di rilievo nazionale "G.RUMMO", ha nominato, con propria delibera n. 320 del 18/02/2005, Titolari del Trattamento dei Dati i Direttori di Dipartimento.
Al Titolare del trattamento competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed alle misure organizzative utilizzate, in materia di privacy, ivi compreso il profilo della sicurezza. Egli si avvale, per il coordinamento delle attività di tutela della privacy, del Referente privacy aziendale, il quale riveste un profilo di carattere esclusivamente funzionale, sia in materia di tutela della privacy che di sicurezza dei dati. Il Titolare del trattamento risponde, in sede penale e civile, degli effetti sanzionatori per mancata ottemperanza alle disposizioni normative sulla tutela della privacy.

Art. 9 – Il Responsabile del trattamento dei dati personali.
I Responsabili del trattamento sono individuati fra soggetti che per esperienza, capacità ed affidabilità possono garantire il pieno rispetto delle vigenti disposizioni in materia di tutela della privacy, ivi compreso il profilo della sicurezza, essi sono stati nominati con atto deliberativo dell'Azienda n. 320 del 18/02/2005, essi sono i Direttori di struttura complessa.
I responsabili del trattamento hanno responsabilità penale, civile ed amministrativa, in materia di privacy.
Responsabile del trattamento è anche il soggetto esterno all'Azienda, che opera in qualità di persona giuridica, sulla base di un rapporto contrattuale di lavoro, in particolar modo, se tale rapporto si esplica in funzione di oneri gestionali e/o di supporto organizzativo.
I compiti del Responsabile del trattamento sono i seguenti:

- Nomina, per iscritto, gli incaricati del trattamento dei dati;
- Impartisce disposizioni organizzative ed operative per il corretto trattamento dei dati e per la sicurezza degli stessi;
- Vigila sulle modalità di trattamento dei dati e sulla correttezza del comportamento del personale incaricato, anche per quanto concerne l'obbligo di tutela della riservatezza e della dignità della persona fisica soggetta a cure, nell'ambito della struttura che egli dirige.

Art. 10 – L'incaricato del trattamento dei dati –
Gli incaricati sono identificati in tutti coloro che materialmente effettuano le operazioni di trattamento di dati. Gli incaricati devono eseguire i trattamenti secondo le disposizioni date dal Responsabile del trattamento, dal quale sono nominati per iscritto ai sensi del precedente art. 9. Nell'atto di designazione sono specificate le istruzioni a cui devono attenersi gli incaricati.

Art. 11 – Il Referente privacy aziendale –
Il Referente privacy aziendale è un Responsabile del trattamento viene nominato dal Direttore Generale con atto deliberativo e delegato dal Titolare del trattamento, a coordinare gli interventi diretti alla tutela della privacy e a verificare l'adozione delle misure di sicurezza nel trattamento dei dati personali. Egli per delega del Titolare del trattamento è preposto:

- ad assolvere all'obbligo di notificazione del trattamento dei dati dell'Azienda, secondo quanto disposto dal Garante per la protezione dei dati personali;
- a redigere modelli atti a fornire l'informativa e ad acquisire il consenso al trattamento dei dati da parte dell'interessato;
- a redigere regolamenti, manuali e codici comportamentali sulla tutela della privacy;
- a richiedere le autorizzazioni per trattamenti non preventivamente autorizzati o ad effettuare le dovute comunicazioni al Garante, in caso di ricorso o di modifica della notifica del trattamento;
- ad adottare, per quanto di competenza, le misure atte a garantire la sicurezza nel trattamento dei dati personali, redigendo ed aggiornando il Documento Programmatico sulla Sicurezza dei dati;
- ad impartire, ai Responsabili del trattamento, le necessarie istruzioni per una corretta gestione dei dati a tutela della privacy, ivi compresa la salvaguardia della loro integrità e sicurezza;
- a diffondere la cultura della privacy in Azienda, mediante la progettazione di interventi formativi in ECM, per i Responsabili e gli incaricati del trattamento.

Il referente privacy aziendale esercita il coordinamento delle su elencate funzioni grazie all'esercizio espletato, in termini progettuali ed operativi, dall'Ufficio Referente privacy.

Art. 12 – L'Ufficio Referente privacy aziendale –
La regolamentazione sulla tutela della privacy sarà attivata dall'Azienda Ospedaliera "G.RUMMO", ai sensi della Legge 675/96 con atto deliberativo del direttore Generale.

In tale atto saranno individuate le funzioni del Referente privacy aziendale, specificatamente dedicato al coordinamento degli interventi diretti alla tutela della privacy nell'Azienda.
Gli sviluppi recenti, in materia di privacy, hanno incrementato il livello di responsabilità e gli oneri progettuali ed organizzativi da parte delle Aziende.
L'Ufficio Referente privacy, pertanto, supporta il Referente privacy aziendale nelle attività elettive con cui egli esplica la sua funzione per delega del Titolare del trattamento.

L'Ufficio Referente Privacy Aziendale dovrà essere costituito da soggetti aventi diverse professionalità:

1. personale amministrativo: soggetti che hanno una qualificata formazione giuridica e conoscono il D.lgs. 196/03, nonché la normativa specifica del settore;
2. personale con competenze gestionali: in considerazione del forte impatto trasversale che la legge ha e richiede la revisione di procedure e il monitoraggio dei flussi informativi in seno all'Azienda e verso l'esterno;
3. personale tecnico-informatico: sono i responsabili e gli operatori del CED. Hanno una formazione tecnica e portano il loro contributo soprattutto in relazione alla valutazione dei rischi e all'adozione delle misure di sicurezza;
4. personale sanitario: chi gestisce gli archivi di dati sanitari ed è responsabile delle strutture e unità.

Le funzioni che possono essere assegnate all'Ufficio, con apposito atto deliberativo del Direttore Generale sono le seguenti:

- assolvere all'obbligo di notificazione del trattamento dei dati dell'Azienda, secondo quanto disposto dal Garante per la protezione dei dati personali;
- redigere modelli atti a fornire l'informativa e ad acquisire il consenso al trattamento dei dati da parte dell'interessato;
- redigere regolamenti, manuali e codici comportamentali sulla tutela della privacy;
- richiedere le autorizzazioni per trattamenti non preventivamente autorizzati o ad effettuare le dovute comunicazioni al Garante, in caso di ricorso o di modifica della notifica del trattamento;
- adottare, per quanto di competenza, le misure atte a garantire la sicurezza nel trattamento dei dati personali, redigendo ed aggiornando il Documento Programmatico sulla Sicurezza dei dati;
- impartire, ai Responsabili del trattamento, le necessarie istruzioni per una corretta gestione dei dati a tutela della privacy, ivi compresa la salvaguardia della loro integrità e sicurezza;
- a diffondere la cultura della privacy in Azienda, mediante la progettazione di interventi formativi in ECM, per i Responsabili e gli incaricati del trattamento.

Art. 13 – Amministratori di sistema –
Il Titolare e i Responsabili del trattamento si avvalgono, nella individuazione e applicazione delle misure necessarie a garantire la sicurezza del sistema informativo, di un amministratore di sistema individuato a tale scopo nel

Responsabile dell'Area funzionale Raccolta ed Elaborazione Dati e sistema informaticò aziendale (CED) o di un suo incaricato formalmente individuato.

Art. 14 – Diritti dell'interessato –

Secondo quanto disposto dall'art. 7 del D.lgs. 196/03, l'interessato ha diritto, redigendo formale richiesta indirizzata all'ufficio del referente privacy, di conoscere:

1. la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione in forma intelligibile;
2. l'indicazione:
   - dell'origine del trattamento dei suoi dati personali;
   - delle finalità e delle modalità del trattamento;
   - della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   - degli estremi identificativi del Titolare;
   - dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati;
3. l'interessato può richiedere:

   - l'aggiornamento, la rettificazione ovvero, qualora vi abbia 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;

4. L'interessato ha inoltre il 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.

Nel caso in cui intenda presentare ricorso, per fatti inerenti al trattamento dei propri dati personali, l'utente dovrà rivolgere istanza scritta all'Ufficio referente privacy aziendale.
L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, in sua vece, delega o procura a persone fisiche o ad associazioni.

Art. 15 – Trattamento di dati affidato all'esterno –

Agli Enti, agli organismi, agli altri soggetti pubblici e privati esterni all'Azienda, ai quali siano affidati attività o servizi, con esclusivo riferimento alle connesse operazioni di trattamento dei dati, viene loro attribuita la funzione di Responsabile del trattamento, ai sensi dell'art. 29 del D.lgs. 196/03.
Nei contratti di affidamento di attività o di servizi a soggetti esterni all'Azienda, può essere inserita apposita clausola di garanzia, con la quale il soggetto affidatario si impegna, per i trattamenti di dati effettuati, in forza del rapporto contrattuale, all'osservanza delle norme di legge sulla protezione dei dati personali.

Art. 16 – Adozione misure di sicurezza informatiche –

1. Con riferimento ai dati elaborati con mezzo elettronico, agli incaricati del trattamento dei dati personali deve essere assegnata una parola chiave per l'accesso ai dati;
2. Nel caso di trattamenti effettuati con elaboratori accessibili in rete sia da altri elaboratori sia mediante una rete di telecomunicazioni ai sensi dell'art. 34 del D.lgs. 196/03, devono essere adottate, le seguenti misure:

    a) A ciascun utente od incaricato del trattamento deve essere attribuito un codice identificativo personale o tecniche di cifrature per l'utilizzazione dell'elaboratore (autentificazione informatica);
    b) Uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
    c) I codici identificativi personali devono essere assegnati e gestiti in modo che non sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore a mesi 6;
    d) Gli elaboratori devono essere protetti contro il rischio di intrusione mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale;
    e) Adozione di procedure per la custodia di copie di sicurezza, il ripristino delle disponibilità dei dati e dei sistemi;
    f) Tenuta di un aggiornato documento programmatico sulla sicurezza.

3. Le disposizioni di cui alle lettere a) e b) non si applicano ai trattamenti di dati personali di cui è consentita la diffusione.
4. Con riferimento ai dati sensibili, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate singolarmente o per gruppi di lavoro, agli incaricati del trattamento con le modalità previste dall'art. 34 del D.lgs. 196/03.

Art. 17 – Documento Programmatico sulla Sicurezza –

Ai sensi degli articoli, da 33 a 36 e dalla regola 19 del Disciplinare Tecnico – Allegato B – , del D.lgs. 196/03, L'Azienda "G.RUMMO" ha redatto ed adottato, con atto deliberativo n. 320 del 18/02/2005, il Documento programmatico della sicurezza dei dati. Tale documento dovrà essere aggiornato annualmente sulla base dell'analisi dei rischi, che emergono dal monitoraggio delle misure logiche, fisiche ed organizzative, adottate dall'Azienda al fine di garantire, in maniera continuativa e migliorativa, la tutela della privacy nel trattamento dei dati e deve contenere idonee informazioni riguardo:

- L'elenco dei trattamenti di dati personali;
- La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- L'analisi dei rischi che incombono sui dati;