Documento Programmatico sulla Sicurezza

Redatto ai sensi e per gli effetti dell'articolo 34. comma 1. lettera g) del D.Lgs. 196/2003 e del disciplinare tecnico (allegato B del D.Lgs. n. 196/2003)

La Medical Center srl titolare di un Poliambulatorio Medico Specialistico Privato Accreditato con sede in Termoli, via Martiri della Resistenza 61/63, P.IVA e COD. FISC. 00997260708

Premesso

che nell'ambito della propria attività effettua trattamento di dati personali, come di seguito elencati, con il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, fisiche e logiche, previste per la tutela dei dati trattati.
In conformità con quanto prescritto al punto 19 del Disciplinare tecnico (allegato B al D.Lgs. 196/2003) nel presente documento si forniscono idonee informazioni riguardanti:

1) Elenco dei trattamenti di dati personali mediante:

1.1) individuazione dei dati personali trattati
1.2) descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
1.3) l'elaborazione della mappa dei trattamenti effettuati

2) Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

3) Analisi dei rischi a cui sono soggetti i dati;

4) Misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati;

5) Criteri e modalità di ripristino dei dati a seguito di distruzione o danneggiamento;

6) Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno;

7) Procedure per il controllo sullo stato della sicurezza;

8) Dichiarazioni d'impegno e firma.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 *Tipologie di dati trattati*

A seguito dell'analisi compiuta si sono identificati i seguenti trattamenti:

- Dati relativi al personale o ai canditati per diventarlo, di natura anche sensibile;
- Dati comuni relativi a clienti e fornitori;
- Dati relativi allo svolgimento di attività economiche e commerciali;
- Dati anche sensibili indispensabili allo svolgimento dell'attività professionale per assolvere a
- obblighi normativi e contrattuali;
- altri …….

1.2 ***Aree, locali e strumenti con i quali si effettuano i trattamenti***

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in Termoli via Martiri della Resistenza 61/63.
Gli uffici sono dislocati al secondo piano del Centro Polifunzionale Lo Scrigno e l'accesso al piano è libero ma controllato da un servizio di guardiania e portierato 24 ore su 24 per 365 giorni all'anno.
L'accesso ai locali del Poliambulatorio è controllato, nell'area della reception e della segreteria dal personale in servizio, nella sala di attesa dall'infermiere e dal personale sanitario in servizio.
L'accesso all'area amministrativa è vietato e l'ufficio è dotato di chiusura a chiave, non in possesso del personale ma solo degli amministratori.

A - Schedari e altri supporti cartacei

I supporti cartacei sono raccolti in schedari a loro volta custoditi come segue:

- Archivio 1 localizzato nei locali della reception e della refertazione ove in appositi armadi vengono archiviati i supporti cartacei di comune e continuo utilizzo;
- Archivio 2 localizzato nel locale amministrativo ove in appositi armadi e in locale al quale accedono solo le persone autorizzate vengono archiviati i supporti cartacei a fine ciclo lavorativo.

B - Elaboratori non in rete

Sono presenti elaboratori non in rete nella Consolle della Tac e nella Consolle della Risonanza Magnetica Nucleare..

C - Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata.
Si dispone di una rete, realizzata mediante collegamenti via cavo costituita da:

- ***n. 1 server, localizzato nell'area accettazione;***
- ***n. 6 postazioni di lavoro dislocate nell'area accettazione, refertazione, studi medici;***
- ***n. 3 stampanti laser dislocate nell'area accettazione, amministrazione e segreteria;***
- ***n. 2 stampanti laser dislocate nelle aree refertazione;***
- ***n. 2 fax localizzati nell'area accettazione/segreteria e in amministrazione;***
- ***n. 1 dispositivo di backup localizzato nell'area accettazione e segreteria;***
- ***n. 2 fotocopiatrici localizzate in Amministrazione e in Accettazione/Segreteria.***

Tipologia trattamento cartaceo	PC	PC		
		Non in rete	In rete priv.	In rete Pubb
Dati comuni relativi a clienti/utenti	x	x	x	
Dati comuni relativi a fornitori	x	x	x	
Dati comuni relativi ad altri soggetti	x		x	
Dati biometrici relativi a clienti/personale	x			
Dati idonei a rilevare la posizione di persone/oggetti				
Dati relativi allo svolgimento di att. econom./comm.	x		x	
Dati di natura giudiziaria	x			
Dati relativi al personale, candidati, anche sensibili	x			
Dati di natura anche sensibile relativi a clienti/utenti	x		x	
Dati idonei a rilevare lo stato di salute	x		x	

Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati emerge che:

1. solo i dati personali vengono trattati sistematicamente con supporti cartacei e con elaborazione;
2. i dati sensibili trattati con elaborazione, sono limitati a quelli necessari per assolvere agli obblighi normativi e contrattuali;
3. i dati giudiziari trattati sono quelli necessari per assolvere agli obblighi normativi e di Legge, essi comunque non vengono trattati con elaborazione;
4. gli elaboratori in rete pubblica presenti, non sono collegati in rete con altri, dispongono esclusivamente del collegamento a internet.

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' ED INTERVENTI FORMATIVI DEGLI INCARICATI

Titolare del trattamento dei dati

Per il trattamento dei dati personali il titolare non ha nominato responsabili, assumendo direttamente l'incarico di progettare, realizzare e mantenere in efficienza le misure di sicurezza.

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua l'ambito del trattamento consentito. Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento. (allegato B)

Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;
- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Formazione degli incaricati al trattamento

Agli incaricati al trattamento, il titolare (direttamente o tramite soggetti da lui identificati) fornisce la necessaria formazione:

- al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansione;
- in occasione dell'introduzione di nuovi strumenti e programmi informatici;

La formazione interesserà sia le norme generali in materia di privacy, sia gli aspetti peculiari dei trattamenti effettuati.

3. ANALISI DEI RISCHI CUI SONO SOGGETTI I DATI

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Strumenti impiegati nel trattamento

Sono stati individuati come sorgenti soggette a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

Strumenti	Legenda
Schedari e altri supporti cartacei custoditi nell'area controllata	A
Elaboratori non in rete custoditi nell'area controllata	B
Elaboratori in rete privata custoditi nell'area controllata	C
Elaboratori in rete pubblica	D

Fattori di rischio	Basso	Medio	Elevato
Rischio d'area legato all'accesso non autorizzato nei locali			A B C D
Rischio guasti tecnici hardware, software, supporti	A B C D		
Rischio penetrazione nelle reti di comunicazione	A B C D		
Rischio legato ad errori umani	A B C D		
Rischio d'area per possibili eventi distruttivi	A B C D		

4. MISURE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

Alla luce dei fattori di rischio e delle aree individuate nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici.

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- misure già adottate al momento della stesura del presente documento;
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente;
- gruppo di continuità dell'alimentazione elettrica;
- impianto di condizionamento.

Sono adottate le misure per impedire accessi non autorizzati.

Custodia e archiviazione dei dati

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso;

Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici;
- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati posso accedere e utilizzare al fine delle proprie mansioni lavorative;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema.

Protezione di strumenti e dati

Premesso che non vengono trattati dati sensibili e giudiziari in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistema firewall anti-intrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.
Agli incaricati è stato affidato il compito di aggiornare comunque periodicamente (ogni mese) il sistema di protezione.

Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in contenitori chiusi a chiave in locali con accesso ai soli autorizzati
- cancellazione e/o distruzione del supporto una volta cessate le ragioni per la conservazione

5. CRITERI E MODALITA' DI RIPRISTINO DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema. Il salvataggio dei dati avviene:

- con frequenza giornaliera;
- le copie vengono custodite in un luogo protetto.

6. AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nello svolgimento dell'attività **non vengono** affidati dati personali all'esterno della Struttura.

7. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il titolare *(il responsabile per la sicurezza)* mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati. Egli verifica, inoltre, con frequenza almeno mensile, l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dati trattati;
- efficacia e utilizzo misure di sicurezza strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti magnetici non più riutilizzabili;
- livello di informazione degli interessati.

8. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data 30.03,2010 viene firmato in calce da Mirella Benedetto in qualità di titolare, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.
L'originale del presente documento è custodito presso la sede della società, per essere esibito in caso di controllo.

Una copia verrà consegnata ai responsabili di determinati trattamenti di dati appositamente nominati.

Termoli 30.03.2010

Firma del Titolare

ORGANIGRAMMA PRIVACY

TITOLARE DEI DATI: **Mirella Benedetto**

RESPONSABILI: **Non nominati**

Soggetti Incaricati del Trattamento sono il Personale Dipendente di Segreteria ed Accettazione per la parte amministrativa e contabile ed il personale sanitario per il trattamento dei dati sanitari e sensibili.

MEDICAL CENTER

Lettera di incarico al trattamento dei dati

Ai sensi del D.Lgs. 196/2003 con la presente La incarichiamo del trattamento dei dati necessari per la gestione, normativa, contabile e previdenziale, nonchè per lo svolgimento dell'attività di gestione amministrativa, aziendale, fiscale e sanitaria della Struttura Medical Center.

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua l'ambito del trattamento consentito.

Istruzioni specifiche sul trattamento dei dati

Le rammentiamo quanto disposto dall'art. 11 del D.Lgs. 196/2003 ex art. 9 legge 675/96.
I dati personali oggetto di 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 raccolti e 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 e successivamente trattati;*

Inoltre si richiede la Sua particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

- *procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;*
- *modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;*
- *modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;*
- *prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;*
- *procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché procedure per il salvataggio dei dati;*
- *modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;*

Modalità operative da seguire per il trattamento dei dati

Al fine della corretta gestione dei dati in trattamento la invitiamo pertanto ad attenersi alle seguenti indicazioni:

- richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa;
- custodire i dati oggetto del trattamento in luoghi non accessibili ai non autorizzati;
- non lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messe in sicurezza dei dati;
- non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni di consultazione;
- custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici;
- accertarsi che i terzi siano a conoscenza e abbiano autorizzato l'uso dei dati richiesti accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
- non fornire telefonicamente o a mezzo fax dati senza specifica autorizzazione e/o identificazione del richiedente;

Le presenti indicazioni sono tassative, la preghiamo di sottoscrivere la presente per presa visione in accettazione di quanto riportato.

Il titolare

Letto firmato e sottoscritto

L'incaricato