Si richiede l'apposizione del timbro postale per la data certa oppure lo si può inviare a se stesso tramite PEC: Data e Firma

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Misure minime di Sicurezza

Ai sensi dell'Art. 34, comma 1, Lettera G e Allegato B – Disciplinare tecnico, regola 19 del decreto legislativo 30 giugno 2003 n. 196

Data : …….

Redatto da:

Riservatezza

Il presente documento è da intendersi ad uso interno e pertanto deve essere trattato come materiale riservato. Non devono essere distribuite copie a terzi

Documento unico formato da n° ……. Pagine . Firma ……

Indice del documento

Premessa

1. Elementi essenziali del modello di attività

1.1 DESCRIZIONE AZIENDA: STUDIO MEDICO

1.2 INFRASTRUTTURA TECNOLOGICA

1.3 TIPOLOGIA DI DATI TRATTATI

1.4 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DEGLI UFFICI PREPOSTI AL TRATTAMENTO

2. Analisi dei Rischi e Misure minime di sicurezza

2.1 METODICA DI ANALISI DEI RISCHI

2.2 PIANO DI FORMAZIONE PER GLI INCARICATI DEL TRATTAMENTO

3. Istruzioni e Procedure per il trattamento di dati personali

3.1 DEFINIZIONI

3.2 TITOLARE DEL TRATTAMENTO

3.3 RESPONSABILI DEL TRATTAMENTO

3.4 AUTORIZZAZIONI

3.5 MODALITÀ DI TRATTAMENTO (ART. 11)

3.6 INFORMATIVE E CONSENSI DELL'INTERESSATO (ART. 13 E ART. 23)

3.7 COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

3.8 DIRITTI DEGLI INTERESSATI

3.9 ESERCIZIO DEI DIRITTI E MODALITA'

3.10 CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI

3.11 TRATTAMENTI AFFIDATI ALL'ESTERNO

4. PIANO DI VERIFICA DELLE MISURE ADOTTATE

5. DISASTER RECOVERY

6 NOMINA INCARICATO

7 LEGENDA OPERATIVA –INFORMAZIONI GENERALI

Premessa

Che cos'è il DPS ?

E' l'unico documento in grado di attestare l'adeguamento della struttura alla normativa sulla tutela dei dati personali. Scopo del DPS è descrivere la situazione attuale (analisi dei rischi, distribuzione di compiti , misure approntate , distribuzione delle responsabilità, elaborazione di un piano di formazione degli incaricati del trattamento) e il percorso prescelto dalla struttura per adeguarsi alla normativa sulla privacy

Adempimenti tecnici per chi adotta schedario cartaceo:

•Proteggere lo schedario cartaceo in un armadio chiuso a chiave
•Proteggere l'accesso al locale dove è custodito lo schedario con misure idonee a scongiurare l'ingresso
•L'accesso agli archivi deve essere controllato; le persone ammesse, dopo l'orario di chiusura, sono identificate e registrate

Il Codice di Tutela dei Dati Personali, emanato con Dpr n. 196 del 30 Giugno 2003, è entrato in vigore il 1 gennaio 2004.

Il Codice riunisce in unico contesto (Testo Unico) la legge madre sulla protezione dei dati (675/1996) e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni, e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche.

Il Testo Unico innova la normativa precedente, in vigore ormai da diversi anni, adeguandola ai mutamenti tecnologici avvenuti ed all'esperienza acquisita, e fornisce, fra l'altro, due indicazioni interessanti:

- viene confermato l'insieme di requisiti che il sistema informativo aziendale deve possedere per fornire un livello minimo di tutela dei dati personali in esso contenuti ("misure minime di sicurezza", presenti in parte nel DPR 318/99)
- si stabilisce che l'insieme così definito di misure non è sufficiente ma è solamente necessario a definire la struttura del sistema ("insieme idoneo di misure" secondo la normativa): l'effettiva struttura deve essere definita caso per caso, come risultante di un processo di analisi che coinvolge l'intero modello di business aziendale.

All'interno del disposto normativo, il Documento Programmatico sulla Sicurezza (DPS) deve contenere gli elementi seguenti:

- 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
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità
- la descrizione dei criteri e delle modalità di ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare
- per i dati personali sensibili, idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato

Nell'analisi sono state fatte le assunzioni seguenti:

- la struttura informativa è analizzata nella configurazione attiva al 01 Giugno 2004
- le sedi dell'azienda sono sul territorio italiano e per questo soggette alle indicazioni contenute nel Codice

Il documento contiene informazioni riservate ed è custodito dal Responsabile del trattamento.

Riferimenti normativi

Decreto Legislativo n. 196 del 30 Giugno 2003, Codice in materia di protezione di dati personali

Decreto del Presidente della Repubblica n. 318 del 28 Luglio 1999, Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2 della legge 31 Dicembre 1996 n. 675

Legge n. 675 del 31 Dicembre 1996, Tutela della privacy, e successive modifiche

1. Elementi essenziali del modello di Attività

1.1 Descrizione attività:

…….

Sede:…….

Città : ……..

C.F.

Tel.

Settore di attività :

Dipendenti n°

Organizzazione Aziendale :

Trattamenti operati dalla struttura:

[X] Strumenti Informatici (Personal Computer)

.

Infrastruttura tecnologica

Dati comuni e sensibili :
Software gestionale :
Supporti di memorizzazione :
Collegamento Internet tramite ADSL [X]

1.2 Tipologia di Dati Trattati

Dati personali :

I dati comuni di cui sopra sono trattati dal titolare del trattamento, dal responsabile e dagli incaricati.

I trattamenti indicati sono esenti dall'obbligo di notifica al Garante ai sensi dell'art. 37 e successivi provvedimenti chiarificatori

Distribuzione dei compiti e delle responsabilità nell'ambito degli uffici preposti al trattamento

1.4 Definizioni dei "Ruoli di Legge e regolamentari"

Di seguito si indicano i ruoli e le competenze per ognuna delle figure previste dal Codice (Art. 4):

- **Titolare**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.
- **Responsabile**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione ed organismo preposti dal titolare al trattamento dei dati personali. I compiti affidati al responsabile sono specificati analiticamente per iscritto.
- **Incaricati**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
- **Interessato**: la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali

2 Analisi dei Rischi e Misure minime di sicurezza

2.1 Metodica di analisi dei rischi

L'analisi del rischio è stata svolta considerando le disposizioni dell'art. 31 del Codice, ovvero i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e trattamento non conforme alle finalità della raccolta.

Le risorse coinvolte nel trattamento dei dati personali sono:

- Luoghi Fisici:
- Risorse hardware/software. :
- Window XP; Microsoft Office

L'Articolo 31 del Codice dispone che i dati personali debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale
- accesso non autorizzato
- trattamento non consentito o conforme alla finalità della raccolta

La sede fisica dell'associazione ha già adottato iniziative volte ad adeguare i sistemi di protezione alle tecnologie attualmente disponibili, per perseguire le finalità di cui sopra
Al fine di assicurare l'integrità dei dati trattati ed impedirne la comunicazione e/o diffusione non autorizzata, l' Associazione Sindacale ha elaborato una precisa Politica di Sicurezza.
Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza a norma, sia un livello idoneo di sicurezza relativamente alle tipologie dei dati trattati , alle modalità di trattamento ed agli strumenti utilizzati.
Accesso Software operativo attraverso password (minimo 8 caratteri)
Accesso Software gestionale attraverso password (minimo 8 caratteri)

Analisi dei Rischi			
Comportamenti degli operatori			
Rischi	Si/No	gravità: alta/media/bassa	Misure adottate
Sottrazione di credenziali di autenticazione	Si	Media	Cod. Identificativo utente più password modificata ogni tre mesi. Cod. identificativo e password non annotate su alcun supporto.
Carenza di Consapevolezza, disattenzione o incuria	Si	Media	Partecipazione a corsi di formazione
Comportamenti sleali o fraudolenti	Si	Media	Controllo diretto dei soggetti incaricati e responsabili del trattamento, istruzione agli stessi
Errore materiale	Si	Media	Idem
Altro evento	No	----------	----------

Errori relativi agli strumenti			
Rischi	Si/No	Gravità: Alta/Media/Bassa	Misure adottate
Azioni di virus informatici o di programmi suscettibili di recare danno	SI	Media	utilizzo di software antivirus specifici, divieto di installazione di ulteriori software senza autorizzazione del titolare, Backup regolare dei dati su supporti esterni eseguite dal titolare.
Spamming o tecniche di sabotaggio	NO	----------	----------
Malfunzionamento, indisponibilità o degrado degli strumenti	SI	Media	Rinnovo della strumentazione.Manutenzione periodica ; Copia di backup dei dati su supporti esterni ai PC
Accessi esterni non autorizzati	SI	Media	Utilizzo di sistemi firewall specifico (Norton Personal firewall); utilizzo di sistema di autenticazione per l'accesso ai dati. Tali procedure sono di competenza del titolare
Intercettazioni di informazioni in rete	NO	----------	----------
Altri eventi	NO	----------	----------

Eventi relativi al contesto			
Rischi	SI/No	Gravita: Alta/Media/Bassa	Misure adottate
Accessi non autorizzati allo studio medico	SI	Media	controllo diretto dei locali da parte del titolare e chiusura a chiave dei locali nel periodo di assenza del titolare e degli eventuali collaboratori.
Sottrazione di strumenti contenenti dati	Si	Media	Custodia e controllo diretto degli strumenti,copia di backup dei dati su supporti esterni al PC
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche, atmosferiche, incendi, allagamenti, condizioni ambientali, ecc…) nonché dolosi, accidentali o dovuti ad incuria.	Si	Bassa	Copia di backup dei dati su supporti esterni al PC
Guasto ai sistemi complementari(impianto elettrico, climatizzazione ecc.)	Si	Media	Copia di backup dei dati su supporti esterni al PC
Errori umani nella gestione della sicurezza fisica	Si	Media	Copia di backup dei dati su supporto esterno,sistema di autenticazione per l'accesso ai dati, istruzioni e controllo dei soggetti incaricati dal titolare a trattare i dati
Altro evento	No	----------	----------

2.2 Piano di formazione per gli incaricati del trattamento

Il piano di formazione deve avere l'obiettivo di istruire e sensibilizzare le risorse incaricate al trattamento nei confronti dei rischi che incombono sui dati stessi, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Il piano è definito come segue: Il titolare dello studio medico ha il compito di provvedere al trattamento dei dati sensibili per le finalità dello stesso; ha il compito di garantire che il trattamento avvenga nel rispetto della legge e dei diritti dell'interessato.

Il collaboratore di studio e/o l'infermiera deve provvedere al trattamento per le finalità proprie della sua mansione attenendosi alle direttive del titolare dello studio.

La formazione sarà effettuata presso lo studio medico con interventi formativi della durata di ore 8 nel corso dell'anno

3 Istruzioni e Procedure per il trattamento di dati personali

A seguito dell'entrata in vigore del Codice in Materia di Protezione dei Dati Personali, lo studio medico in oggetto è tenuto a conformarsi con il dettato della legge, e ne chiede il rispetto a tutti i collaboratori.

A tale scopo si dispone che i dati personali contenuti nelle banche dati e negli archivi cartacei dello studio medico debbano essere trattati in conformità a quanto previsto dal Documento Programmatico di Sicurezza, che contiene le istruzioni nonché i criteri tecnici e le procedure organizzative richieste dalla legge.

Tali istruzioni e procedure dovranno essere osservate dagli Incaricati nello svolgimento delle operazioni di trattamento dei dati personali.

3.1 Definizioni

Ai fini del presente documento si specificano le seguenti definizioni:

Definizioni come da Art. 4 del Codice

Trattamento, qualunque operazione o complesso di operazioni , effettuate 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;

Dato Personale, 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;

Dati Identificativi, i dati personali che permettono l'identificazione dell'interessato;

Dati Sensibili, i dati personali idonei 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 rilevare lo stato di salute e la vita sessuale.

Titolare, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza;

Responsabile, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Incaricati, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato, la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali;

Comunicazione, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Dato Anonimo, il dato che in origine o a seguito di trattamento non può essere associato ad un interessato identificato o identificabile;

Blocco, la conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca Dati, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

Comunicazione elettronica, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

Misure minime, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

Autenticazione informatica, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

Credenziali di autenticazione, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

Parola Chiave, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

Profilo di Autorizzazione, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

Sistema di Autorizzazione, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Definizioni aggiuntive

Uffici Operativi : .

Responsabile degli Uffici Operativi: il titolare, il responsabile e gli incaricati.

Amministratore dei Sistemi : il titolare, il responsabile e gli incaricati

Gestore delle Password : Il titolare, il responsabile e gli incaricati.

3.2 Titolare del Trattamento

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da qualsiasi altro ente, associazione od organismo, Titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Titolare è tenuto a vigilare anche tramite verifiche periodiche sulla puntuale osservanza delle disposizioni e delle proprie istruzioni in materia di trattamento seguite dal Responsabile.

3.3 Responsabili del Trattamento

Il Responsabile del Trattamento, designato facoltativamente dal Titolare, provvede e vigila, in conformità alle istruzioni ricevute e alla legislazione vigente, affinché siano rispettate le disposizioni del Codice.

Il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario, per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal titolare, e devono essere specificati al minimo i seguenti argomenti:

- obblighi di ordinaria diligenza a cui è tenuto a conformarsi il Responsabile
- eventuali regole per le nomine degli incaricati
- eventuali regole da seguire nel caso di autorizzazioni preventive all'utilizzo di dati personali comuni e sensibili da parte di incaricati.
- eventuali regole da seguire nel caso di autorizzazioni preventive all'utilizzo di dati personali comuni e sensibili da parte di incaricati.
- regole per predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni dell'art. 31 del D.Lgs 196 del 30 giugno 2003.

3.4 Incaricati del Trattamento

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

Possono essere incaricati per iscritto i soli dipendenti e i collaboratori che debbano trattare i dati personali per ragioni attinenti allo svolgimento delle proprie mansioni.

Ogni dipendente o collaboratore dello studio medico che per mansioni assegnate debba trattare dati personali deve essere incaricato per iscritto in conformità alle procedure previste dal Codice e indicate nel presente Manuale. La lettera di incarico conferita deve essere redatta in conformità ai modelli predisposti.

Come indicato nell'art. 30, sono previste anche nomine di gruppo per gli incaricati appartenenti allo stesso ufficio o unità operativa. In tal caso, ciascuna delle persone nominate apporrà una firma di ricevuta su un unico documento, contenente tutti i nominativi "omogenei". Le istruzioni operative possono essere fornite a parte, diversificandole se necessario per ciascuno dei soggetti nominati incaricati. Tali istruzioni dovranno contenere indicazioni sui seguenti argomenti:

- regole per l'accesso ai dati dalla postazione di lavoro
- modalità d'uso e di gestione della propria password
- aggiornamento dell'antivirus
- modalità per il salvataggio dei dati

- uso e restituzione dei supporti di memorizzazione dei dati
- accesso ad archivi cartacei e modalità di conservazione delle cartelle e/o dei documenti
- regole per l'utilizzo degli strumenti di comunicazione elettronica
- uso di fax, stampanti

Nuove assunzioni. Ad ogni assunzione di nuovo personale addetto allo studio medico, il Titolare provvede a consegnare al nuovo Incaricato, unitamente a tutti gli altri documenti aziendali previsti, l'informativa di gruppo contenente la descrizione delle mansioni di trattamento, richiedendo contestualmente la firma di ricevuta della stessa.

3.4 Autorizzazioni

Per ragioni di controllo in merito alla regolarità, veridicità e aggiornamento della documentazione privacy utilizzata, il Responsabile del Trattamento autorizza l'avvio dei nuovi trattamenti.

I Dati Sensibili possono essere trattati solamente da Incaricati appartenenti allo studio medico autorizzati per iscritto in tal senso dal Responsabile del trattamento.

Le autorizzazioni devono essere redatte in conformità al modello predisposto dal Responsabile del trattamento. L'autorizzazione deve limitare l'accesso degli incaricati ai soli dati necessari e sufficienti allo svolgimento delle mansioni cui sono preposti gli Incaricati.

Tali autorizzazioni devono inoltre indicare gli elaboratori con cui è possibile accedere ai Dati Sensibili per effettuare operazioni di trattamento, nonché eventuali strumenti utilizzati per interconnessione. Il titolare provvede a redigere e conservare, aggiornandolo, un elenco degli elaboratori assegnati agli Incaricati appartenenti allo studio medico autorizzati al trattamento di dati sensibili.

3.5 Modalità di Trattamento (art. 11)

Il trattamento deve essere effettuato nel rispetto delle norme di legge, delle disposizioni di cui al presente Manuale, secondo le direttive o istruzioni impartite dal Responsabile del trattamento, dai Responsabili degli Uffici Operativi e dall'Amministratore dei Sistemi.

Il trattamento deve essere effettuato esclusivamente per gli scopi determinati nelle lettere di Incarico, unici scopi legittimi per i quali i dati personali possono essere trattati. Per ogni categoria di Interessato, tali scopi devono essere esplicitati nelle apposite informative predisposte che dovranno essere consegnate a ciascun Interessato.

Il Responsabile del trattamento, i Responsabili degli Uffici Operativi, l'Amministratore dei Sistemi e gli Incaricati devono fare quanto ragionevolmente necessario per assicurare che i dati personali oggetto dei trattamenti siano esatti e se necessario aggiornati.

I dati personali oggetto dei trattamenti devono essere pertinenti, completi e non eccedenti rispetto alle finalità per cui sono raccolti e trattati. Agli Incaricati è rimesso il compito di

valutare, con criterio di ragionevolezza, le suddette caratteristiche dei dati personali raccolti e trattati. Ai Responsabili degli Uffici Operativi è rimesso il compito di vigilare circa il rispetto della presente norma regolamentare.

I dati personali oggetto dei trattamenti devono essere 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, salvo il rispetto di obblighi di legge che determinino obblighi di legge più lunghi.

In tutti i casi, i dati personali non possono essere utilizzati per scopi illeciti o incompatibili con i fini per i quali sono stati raccolti e registrati.

3.6 Informative e Consensi dell'Interessato (art. 13 e art. 23)

Informativa

Al momento della raccolta dei dati personali, all'Interessato deve essere data preventiva informativa orale o scritta circa:

1. le finalità e le modalità del trattamento cui sono destinati i dati;
2. la natura obbligatoria o facoltativa del conferimento dei dati;
3. le conseguenze di un eventuale rifiuto di rispondere;
4. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
5. i diritti dell'interessato di cui all'art. 7 del Codice
6. gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile

La disposizione non si applica quando:

1. i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
2. i dati sono trattati ai fini dello svolgimento di investigazioni difensive o comunque per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

. l'informativa all'interessato comporta un impiego di mezzi che il Garante dichiari manifestamente sproporzionati rispetto al diritto tutelato oppure si riveli impossibile.

Sulla base del nuovo Codice, l'Informativa può essere trasmessa, oltre che in forma scritta, in forma orale (es. nel caso di Call Center o sistemi di risposta automatica) e con forme e tecniche semplificate (pieghevoli o cartoncini riassuntivi).

Consenso

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato, che può riguardare l'intero trattamento oppure una o più operazioni, deve essere espresso liberamente, in forma specifica e documentata per iscritto ed a seguito dell'informativa di cui all'art. 13.

Il consenso non è richiesto quando il trattamento:

1. è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

2. è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

3. riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

.4 riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

5. è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;

6. con esclusione della diffusione, è necessario ai fini dello svolgimento di investigazioni difensive o comunque per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

7. con esclusione della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti;

8. è necessario in conformità ai rispettivi codici di deontologia, per esclusivi scopi scientifici, storici o statistici.

3.7 Comunicazione e Diffusione dei dati personali

I dati personali possono essere comunicati esclusivamente:

1. ad Incaricati di altri Studi medici che per mansioni possano trattare tali dati;
2. a soggetti rispetto ai quali è previsto un obbligo normativo di comunicazione;
3. a soggetti rispetto ai quali la comunicazione è necessaria per adempiere ad un obbligo contrattuale previsto da accordi di cui è parte l'interessato;
4. quando vi sia il consenso dell'Interessato o degli Interessati;
5. qualora i dati provengano da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
6. quando la comunicazione sia necessaria ai fini dello svolgimento di investigazioni penali o per far valere o difendere un diritto in sede giudiziaria.

In ogni altro caso è vietata la comunicazione di dati personali a soggetti non appartenenti allo studio medico.

E' vietata qualsiasi forma di diffusione dei dati personali, salvo consenso scritto dell'Interessato.

3.8 Diritti degli Interessati

Gli articoli da 7 a 10 del Codice sanciscono l'insieme dei Diritti che l'Interessato può far valere rispetto al trattamento dei propri dati personali. In particolare, l'art. 7 stabilisce:

- conferma o meno dell'esistenza di dati personali che riguardano l'Interessato
- indicazione dell'origine dei dati, della finalità e modalità del trattamento, della logica applicata nel trattamento con strumenti elettronici, degli estremi identificativi del Titolare e del Responsabile del trattamento, dei soggetti a cui i dati possono essere comunicati;

- diritto di ottenere l'aggiornamento, rettifica o integrazione dei dati; la cancellazione, trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge; l'attestazione dell'avvenuto adempimento degli obblighi per la comunicazione o diffusione dei dati
- possibilità di opposizione al trattamento dei dati a fini di informazione commerciale, invio di materiale pubblicitario, di vendita diretta e per il compimento di ricerche di mercato

3.9 Esercizio dei diritti e modalità

I diritti sanciti dall'art. 7 possono essere esercitati con richiesta diretta al Responsabile del trattamento o all'Incaricato senza particolari formalismi.

Si specifica nell'art. 8 del Codice che l'esercizio dei diritti può avere luogo salvo che concerna la rettificazione o integrazione di dati personali di tipo valutativo, relativi a giudizio, opinioni o altre informazioni di tipo soggettivo, così come indicazioni relative alla condotta da tenere o decisioni prese in via di assunzione da parte del titolare del trattamento.

3.10 Cifratura dei dati o separazione dei dati identificativi

Trattamento dati: vengono trattati dati comuni contenuti nella banca dati FIMP Treviso.

Protezione scelta: Cifratura proprietaria del programma prevista dalla software house

Descrizione: dati comuni anagrafici

3.11 Trattamenti affidati all'esterno : nessuna attività esterna

4 Piano di verifica delle Misure Adottate

La bontà delle misure adottate deve essere periodicamente verificata.

Durante queste operazioni di verifica, da effettuarsi al più ogni sei mesi, sarà data particolare importanza a :

1) Verifica della bontà delle misure anti-intrusione adottate.
2) Corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati, con particolare attenzione alla disattivazione dei codici di accesso non utilizzati per più di sei mesi3
3) Aggiornamento dei programmi software che trattano i dati personali.
4) Integrità dei dati e delle loro copie di backup.
5) Bontà di conservazione dei documenti cartacei.
6) Accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati.
7) Accertamento del livello di formazione degli incaricati. Prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda.

Di queste verifiche sarà redatto un verbale che potrà essere allegato al documento programmatico sulla sicurezza.

5 Disaster Ricovery

Misure di sicurezza adottate:

Copia di backup dei dati su supporto esterno allo strumento (Floppy Disk; Pen Drive, Disco Di memoria esterno ecc..)

Personale addetto al backup : Responsabile del trattamento e gli incaricati

I supporti esterni di backup sono custoditi dal responsabile del trattamento dati.

Il sistema di utilizzo del backup : software operativo Window XP e Microsoft Office.

Il sistema di ripristino : tramite software gestionale installato

Sono effettuate prove di ripristino periodiche per valutare la funzionalità del sistema.

Personale addetto al ripristino : il titolare dello studio medico

Data redazione del documento :

Firma del titolare del trattamento dei dati dott.

Firma del Responsabile del trattamento dei dati :

NOMINA A INCARICATO TRATTAMENTO DATI

Gentile a

Ai sensi del D.Lgs 196 del 30 giugno 2003 con il presente atto Le conferiamo l'incarico di trattare i Dati personali aziendali relativi allo svolgimento delle mansioni a Lei affidate, in conformità alla legge ed alle istruzioni impartite dal titolale o dal responsabile del trattamento.

Si intende "trattamento" qualsiasi operazione, o insieme di operazioni, eseguite o meno tramite supporti informatici, che registri, organizzi, conservi, elabori, modifichi, comunichi, diffonda, cancelli e distrugga tali dati e la loro relativa sicurezza.

In particolare, nello svolgimento delle Sue mansioni, La autorizziamo a trattare Dati Personali riferiti alle seguenti categorie di Interessati:

Pazienti afferenti allo studio medico

I dati personali potranno da Lei essere trattati sia a livello cartaceo sia informatico, attraverso l'utilizzo di software e banche dati informatiche cui Lei avrà accesso tramite le Sue User ID e password, nonché tramite l'accesso a documenti custoditi in archivi ad accesso selezionato cui Lei sarà abilitato ad accedere.

I suoi incarichi relativi al Trattamento prevederanno di:

- raccogliere e registrare i dati personali
- verificare la completezza e correttezza dei dati personali in sede di raccolta e registrazione procedendo all'eventuale aggiornamento, rettifica o integrazione degli stessi
- procedere al rilascio dell'informativa all'interessato ed alla richiesta del consenso dello stesso, se ed in quanto necessario ai sensi della legge
- verificare che i dati personali siano pertinenti e non eccedenti le finalità per le quali essi sono trattati, nonché procedere alla cancellazione, trasformazione in forma anonima o al blocco dei dati personali trattati in violazione della legge, secondo le istruzioni impartite dal titolare o dal responsabile del trattamento
- conservare i dati personali rispettando le misure di sicurezza di cui all'art. 31/DLgs 196 e quelle individuate nel relativo Disciplinare (Allegato B/DLgs 196)
- fare quanto necessario per impedire l'accesso ai dati personali da parte di terzi, compresi altri dipendenti della Società, anche in caso di allontanamento temporaneo dal proprio posto di lavoro.

Nessun dato potrà essere comunicato a terzi, compresi altri dipendenti della Società, né trasferito all'estero senza la preventiva autorizzazione del titolare o del responsabile del trattamento.

Data…

Per conferma ed accettazione:

RTD

ITD

NOMINA A INCARICATO TRATTAMENTO DATI IN AMBITO FORME ASSOCIATIVE O SOSTITUTI

Gentile Dott. Dott.

Dott. Dott.

Dott. Dott.

Ai sensi del D.Lgs 196 del 30 giugno 2003 con il presente atto Le conferiamo l'incarico di trattare i Dati personali aziendali relativi allo svolgimento delle mansioni a Lei affidate, in conformità alla legge ed alle istruzioni impartite dal titolale o dal responsabile del trattamento.

Si intende "trattamento" qualsiasi operazione, o insieme di operazioni, eseguite o meno tramite supporti informatici, che registri, organizzi, conservi, elabori, modifichi, comunichi, diffonda, cancelli e distrugga tali dati e la loro relativa sicurezza.

In particolare, nello svolgimento delle Sue mansioni, La autorizziamo a trattare Dati Personali riferiti alle seguenti categorie di Interessati:

Pazienti afferenti allo studio medico

I dati personali potranno da Lei essere trattati sia a livello cartaceo sia informatico, attraverso l'utilizzo di software e banche dati informatiche cui Lei avrà accesso tramite le Sue User ID e password, nonché tramite l'accesso a documenti custoditi in archivi ad accesso selezionato cui Lei sarà abilitato ad accedere.

I suoi incarichi relativi al Trattamento prevederanno di:

- raccogliere e registrare i dati personali
- verificare la completezza e correttezza dei dati personali in sede di raccolta e registrazione procedendo all'eventuale aggiornamento, rettifica o integrazione degli stessi
- procedere al rilascio dell'informativa all'interessato ed alla richiesta del consenso dello stesso, se ed in quanto necessario ai sensi della legge
- verificare che i dati personali siano pertinenti e non eccedenti le finalità per le quali essi sono trattati, nonché procedere alla cancellazione, trasformazione in forma anonima o al blocco dei dati personali trattati in violazione della legge, secondo le istruzioni impartite dal titolare o dal responsabile del trattamento
- conservare i dati personali rispettando le misure di sicurezza di cui all'art. 31/DLgs 196 e quelle individuate nel relativo Disciplinare (Allegato B/DLgs 196)
- fare quanto necessario per impedire l'accesso ai dati personali da parte di terzi, compresi altri dipendenti della Società, anche in caso di allontanamento temporaneo dal proprio posto di lavoro.

Nessun dato potrà essere comunicato a terzi, compresi altri dipendenti della Società, né trasferito all'estero senza la preventiva autorizzazione del titolare o del responsabile del trattamento.

Data……..

Per conferma ed accettazione:

RTD ……

ITD ……

Legenda operativa:

Informazioni generali in materia di Privacy

Il Consiglio dei Ministri (n. 37 del 22 dicembre 2005) ha stabilito di prorogare la compilazione del Documento Programmatico di Sicurezza (DPS) dal 31 dicembre 2005 al 31 marzo 2006. Nello specifico il decreto cosiddetto “Milleproroghe” approvato dal Consiglio dei Ministri ha ridisegnato il calendario degli adempimenti previsti dagli articoli 180 e 181 del Codice della Privacy.
L’articolo 180 distingue tra misure minime di sicurezza **vecchie** (quelle previste dal DPR n. 318/1999) e **nuove** (quelle previste dall’allegato B al Codice) . Pertanto stando all’interpretazione letterale del decreto , **solo le nuove** misure minime di sicurezza usufruiscono della proroga.
Poiché l’Autorità Garante della Privacy , con motivato parere del 22 marzo 2004 , ha espressamente interpretato come misura nuova la redazione del DPS , di conseguenza la sua compilazione è prorogata al 31 marzo 2006.
Attenzione quindi alle misure minime di sicurezza **vecchie, quelle cioè previste dal DPR n. 318/1999,** che devono già essere in atto al momento della redazione del DPS.
Queste sono costituite dall’insieme degli accorgimenti tecnici e governativi che il titolare (in questo caso il **medico**) di un trattamento di dati personali deve adottare per assicurare il livello minimo di sicurezza dei dati personali. Tra esse si considerano:

- l’obbligo di adottare un sistema di autentificazione informatica (password) ed un sistema di autorizzazioni;
- la necessità di proteggere i dati personali contro i rischi di intrusione (installazione di firewall) e di azioni di programmi dannosi quali per es. virus informatici(installazione di antivirus con obbligo di aggiornamento periodico)
- L’obbligo di prevedere aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici
- La necessità di adozione di procedure per la custodia di copie di sicurezza dei dati e per il ripristino della disponibilità degli stessi e dei sistemi (piano di disaster recovery)
- La necessità di adottare tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rilevare lo stato di salute effettuati da organismi sanitari.

RISPETTATE LE REGOLE CHE VOI STESSI AVETE DICHIARATO.

Se avete scritto, per es., che il computer e' protetto da password e che tale password e' conosciuta solo dall' interessato, deve essere effettivamente cosi'

.
QUESTO DOCUMENTO NON VA SPEDITO.

Va conservato in studio per eventuali controlli.
- **DEVE AVERE DATA CERTA**, e' consigliabile attribuire una data certa, anche perche' e' una procedura non difficile.
- **COME SI FA?** : e' possibile far timbrare il documento all' ufficio postale o oppure spedirlo a se stessi con raccomandata o PEC, conservandola poi chiusa.
- **PER QUANTO TEMPO VA CONSERVATO?** Indefinitamente, se non ci sono variazioni da registrare; in caso di variazione della situazione locale occorre stilare un nuovo documento, ma e' bene conservare anche quello vecchio e far riferimento ad esso.

VANNO COMPILATI ALTRI DOCUMENTI? : occorre far firmare al personale la dichiarazione di avvenuta formazione (che sono stati informati e "formati" sulle procedure da rispettare per la tutela, custodia e protezione dei dati ad essi affidati).

Per capire meglio le procedure ricordate che:
- L' amministratore di sistema e' colui che, nel caso di computer collegati in rete, gestisce la rete stessa, le password dei vari medici ecc. (ciascun medico deve conoscere SOLO la propria password, l' amministratore e' l' unico che le conosce tutte).
- Il Titolare dei dati e', in genere, il medico stesso.
- Il Responsabile e' ancora il medico, a meno che non abbia affidato la responsabilita' ad una ditta o simili.
- L' Incaricato e' colui che, dietro incarico del medico, accede ai dati dei pazienti (segretaria, sostituto, tirocinante ecc...**N. B**. Gli associati sono "titolari" e "responsabili" dei propri dati, e devono compilare ciascuno il proprio DPS, ma sono "incaricati" per quanto riguarda i dati degli altri medici).
- Questi soggetti non vanno indicati nominativamente ma in modo generico (l' ha detto il Garante in una riunione presso un Sindacato), pero' a ciascuno di essi va dato un foglio di incarico scritto (trattenendone una copia firmata per ricevuta). Questo e' necessario perche' il medico possa respingere delle responsabilita' qualora un incaricato ecceda dai suoi compiti o compia qualche violazione.

RTD = Responsabile trattamento dati

ITD = incaricato trattamento dati