



Documento Programmatico sulla sicurezza

Redatto ai sensi dell'articolo 34, comma 1, lettera g) e Allegato B - Disciplinare Tecnico, Regola 19 del Decreto legislativo 30 Giugno 2003 n.196 "Codice in materia di protezione dei dati personali"

Firma del Titolare del trattamento dei dati: _____

Firma del Responsabile del trattamento dei dati: _____

Data redazione documento _____

Scopo del documento

Scopo di questo documento è delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche adottate e da adottare per il trattamento dei dati personali effettuato dal titolare e dal responsabile dei dati (se nominato)

Premessa

Il presente documento, in ottemperanza alle prescrizioni del D.Lgs. n. 196/2003 ("Codice della Privacy"), individua le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema informatico descritto nel presente documento deve ritenersi sicuro in quanto strutturato secondo quanto previsto e richiesto dalla normativa per garantire la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

Conformemente a quanto prescrive il punto 19. del Disciplinare Tecnico, allegato sub b) al D.Lgs. 196/2003, la stesura del presente documento è aderente alle seguenti linee guida:

1. l'elenco dei trattamenti di dati personali effettuato;
2. l'analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento;
3. l'individuazione e la valutazione dei rischi che incombono sui dati;
4. l'individuazione delle misure preventive e correttive, già adottate o 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;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei dati o degli strumenti elettronici,
6. l'individuazione di istruzioni agli incaricati e la previsione di un programma formativo;
7. i criteri da adottare per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
8. i criteri di cifratura o separazione dei dati

ADEMPIMENTI E SCADENZE ALLEGATO B

- Ogni settimana: Attivare la procedura di salvataggio dei dati sensibili e personali dei pazienti



- Ogni tre mesi: Modificare la password
- Ogni sei mesi: Attivare gli strumenti di protezione dei dati degli assistiti - Aggiornare i programmi antivirus
- Ogni anno: Verificare le funzioni attribuite agli incaricati - Compilare il documento programmatico sulla sicurezza - Programmare interventi di formazione per gli incaricati del trattamento.

ANAGRAFICA

Titolare del trattamento dei dati Dott. _____

Domicilio Fiscale Indirizzo: _____

Sede professionale dove avviene il trattamento dei dati

Indirizzo: _____

Codice fiscale: _____

Partita IVA : _____

Tipo di attività professionale esercitata Medico di Medicina Generale

Dati ASL ASL riferimento _____

Tipologia organizzativa Studio singolo
Studio associato
Medicina in rete
Medicina in Gruppo

Responsabile del trattamento dei dati (se diverso dal titolare)

Cognome e nome _____

Data nomina per iscritto _____

In tale studio operano inoltre i seguenti Medici:

Dott. _____

Dott. _____

Dott. _____

Dott. _____

Tali medici operano in regime associativo, con possibilità di trattare, nelle forme consentite e con il consenso degli interessati, i dati personali e sensibili dei pazienti di ciascun associato.



Altri soggetti autorizzati al trattamento dei dati: Collaboratori/dipendenti

Nome _____

Ruolo _____

Tratta i dati sì
 no

Nome _____

Ruolo _____

Tratta i dati sì
 no

Il medico tirocinante

Tratta i dati sì
 no

Il Medico Sostituto

Tratta i dati sì
 no

Tipologia dei dati:

dati personali dei soggetti che si rivolgono al medico per fini di diagnosi e cura, o per altri fini attinenti la salute dell' interessato e/o per ogni incombenza che la legge attribuisce ai laureati in Medicina.

Tipologia del trattamento dei dati

Schedario cartaceo
Strumenti elettronici
Entrambi

INFORMAZIONI SUL SISTEMA INFORMATIVO BACKUP E RIPRISTINO DEI DATI

Numero di computer utilizzati [__]

Di cui collegati ad Internet N°: [__]

Copie di sicurezza

Le copie di sicurezza dei dati sono effettuate su:

tutti i Pc sì
 no
solo sul server

Le copie di sicurezza dei dati sono effettuate con periodicità:

Giornaliera
Settimanale
Altro



Il sistema operativo dei PC è aggiornato periodicamente con le patch fornite dal produttore?

- si
- no

Ripristino dei dati

Periodicità delle prove di ripristino dei dati:

- Settimanale
- Mensile
- Altro

SICUREZZA ALL'ACCESSO DEI DATI

Accesso dei dati al computer principale

L'accesso ai dati custoditi sul computer principale è coperto da chiavi personali

- USERID si
 no

- Password si
 no

Accesso dei dati agli altri computer

- E' necessario fornire USERID e PASSWORD su tutti i PC si
 no

Modifica delle password

- Giornaliera
- Settimanale
- Mensile
- Altro

Tipologia delle password

- Diverse per ogni operatore/collaboratore si
 no

- La password è lunga almeno 8 caratteri si
 no

Antivirus

- Il PC principale dispone di un software antivirus si
 no
- Gli altri PC dispongono di un software antivirus si
 no

Il sistema antivirus è aggiornato con le patch fornite dal produttore

- Giornaliera
- Settimanale
- Mensile



Altro

Sistemi firewall

I sistemi sono protetti da firewall? sì
 no

Posta elettronica

Utilizzo la posta elettronica sì
 no
su tutti i Pc sì
 no
solo sul Pc principale

SICUREZZA FISICA DEI LOCALI

I locali sono dotati di

Porta blindata sì
 no
Tapparelle blindate sì
 no
Inferiate sì
 no

Gli armadi / casseti

Gli armadi ed i casseti dove sono custoditi i dati su supporto cartaceo sono dotati di serratura sì
 no

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Analisi dei rischi

Tipologia Livello Rischio

RISCHI AMBIENTALI

basso (incendio, terremoto, inondazione) medio alto

RISCHI ORGANIZZATIVI

basso (furto, uso illegittimo dei dati) medio alto

RISCHI FISICI (danneggiamento volontario, basso Involontario, guasti interruzione d'uso) medio alto

RISCHI LOGICI (accesso esterni non autorizzati, basso azione virus, cancellazione dati, invio e-mail a medio indirizzi sbagliati) alto

Tutto il personale operante nello studio è informato e formato riguardo al corretto trattamento dei dati personali dei pazienti, nonché delle responsabilità che ne possano derivare. Gli incaricati sono adeguatamente istruiti per non lasciare incustoditi e accessibili lo strumento elettronico e/o il materiale cartaceo, durante l'orario di apertura dello studio.