d Demetra®
centro medico

Studio medico polispecialistico
di **NOVAN S.R.L**
Via Umberto Pavoni, 10 - Grottaferrata
P.IVA: 04452921002
Aut.Reg.Lazio n.G14405 del 23/11/2015

Grottaferrata, gennaio 2020

REGISTRO DEL TRATTAMENTO DEI DATI

1. *il titolare del trattamento dei dati personali è la NOVAN SRL con sede in Grottaferrata Via Umberto Pavoni n.10, P.Iva 04452921002 nella persona del Direttore Sanitario della struttura Dott.ssa Novella Russo che sovrintende le attività dei singoli medici professionisti esercenti la attività libero professionale, tutti domiciliati per la funzione presso la sede sopra indicata;*

2. *le finalità e le modalità del trattamento cui sono destinati i dati, sono quelle connesse con le attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico a tutela della salute dell'interessato nell'ambito della corretta attività medico professionale;*

3. *per il raggiungimento delle finalità di cui sopra, i dati raccolti devono intendersi come dati sensibili in quanto riguardano gli elementi costituenti la salute del soggetto interessato;*

4. *i dati saranno custoditi per tutto il periodo di durata della prestazione sanitaria e saranno conservati fino al compimento del decimo anno dalla erogazione della ultima prestazione.*

5. *i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati (medici sostituti, laboratorio analisi, medici specialisti, farmacisti, aziende ospedaliere, case di cura private e fiscalisti ovvero soggetti governativi per adempimenti normativi) o che possono venirne a conoscenza in qualità di incaricati (personale amministrativo dello Studio Medico Polispecialistico indicato al punto 1);*

6. *l'interessato può chiedere l'accesso ai propri dati, la rettifica, la cancellazione (diritto all'oblio) e la portabilità degli stessi (diritto dell'interessato di trasmettere ad altro titolare del trattamento i propri dati personali, senza impedimenti dal primo titolare);*

7. *l'interessato può revocare in ogni momento il proprio consenso;*

8. *l'interessato può fare ricorso al Garante della privacy in caso di violazioni;*

9. *la mancata comunicazione dei dati personali da parte dell'interessato comporta l'impossibilità di eseguire la prestazione sanitaria, essendo quest'ultima diretta conseguenza della elaborazione dei dati personali dell'interessato;*

10. *i dati non verranno elaborati con processo decisionale automatico e/o profilazione.*

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
PUNTO I
INDIVIDUAZIONE DEI DATI TRATTATI

I dati trattati dai titolari vengono così classificati:

- dati comuni relativi ai clienti;
- dati comuni relativi ai fornitori;
- dati comuni relativi ad altri soggetti esterni;
- dati comuni relativi ai dipendenti ed assimilati;
- dati sensibili relativi ai clienti;

I dati vengono trattati nell' esclusivo svolgimento delle finalità istituzionali dell' attività Medica.

PUNTO II

CRITERI TECNICI ED ORGANIZZATIVI PER LA PROTEZIONE DELLE AREE E DEI LOCALI INTERESSATI DALLE MISURE DI SICUREZZA E PROCEDURE PER CONTROLLARE L'ACCESSO DELLE PERSONE AUTORIZZATE AI LOCALI MEDESIMI.

Il trattamento dei dati avviene nello studio sito in Grottaferrata.
I locali sono protetti contro il rischio di intrusione dalla presenza di tre porte protette da inferriate munite di chiavi in possesso anche del personale dipendente.
Lo studio osserva il seguente orario:

Dal lunedì al venerdì dalle ore 9.30 alle ore 19.30

Le "aree di accesso controllato" dello studio medico, a cui le persone non autorizzate al trattamento dei dati personali (estranei , clienti , collaboratori , non addetti al trattamento) avranno accesso solo se accompagnati da un addetto o sotto il controllo (anche solo visivo) di uno o più addetti sono :
Tutto lo studio ad eccezione di :

- **Ingresso – sala d’aspetto**
- **Toilettes.**

È’ comunque interdetto l’accesso alle “aree ad accesso controllato“ in orario diverso da quello di lavoro, se non previa autorizzazione esplicita scritta e/o verbale del titolare.

Le aree di accesso controllato contengono: computers, stampanti, Fax, server, dispositivo di backup installato all’interno del server e archivi cartacei.

E non è quindi consentito ad estranei di leggere od asportare alcun documento o informazioni all' insaputa degli incaricati al trattamento .

Le persone autorizzate al trattamento e responsabili della custodia dei dati personali sono quelli indicati al punto 1 oltre agli altri medici specialisti e/o professionisti eventualmente interessati al trattamento dei dati nel corso della espletazione della prestazione sanitaria.

PUNTO III

CRITERI E PROCEDURE PER ASSICURARE L’INTEGRITA’ DEI DATI.

Se nelle “aree ad accesso controllato“ sono presenti persone non autorizzate al trattamento dei dati personali e non vi è alcuna persona a sorvegliare, i sistemi informatici vengono disattivati o spenti o viene attivato uno screen-saver dotato di password. Tale screen-saver viene automaticamente attivato dopo cinque minuti di inattività del computer.

Se nelle aree ad accesso controllato sono presenti persone non autorizzate al trattamento dei dati personali e non vi è alcuna persona a sorvegliare , i documenti cartacei contenente dati personali vengono riposti in una apposita custodia munita di serratura.

I computer non vengono mai lasciati accesi ed incustoditi.

Fax e server di sistema sono collocati in aree di accesso controllato o comunque non visibili al personale non addetto al trattamento dei dati ed al pubblico - non è quindi possibile ad estranei leggere o asportare documenti non ancora prelevati dal personale.

È vietato far accedere al sistema personale non espressamente autorizzato dai titolari.

Tutte le persone, autorizzate per iscritto al trattamento dei dati personali, sono dotate di un user-id (identificatore) di accesso al sistema informatico che devono confermare tramite password. Non è possibile accedere in più persone con la stessa user-id. Le password vengono modificate ogni 6 mesi.

I codici identificativi personali sono stati assegnati e gestiti in modo che ne sia prevista la disattivazione nel caso in cui l'incaricato perda la qualità che gli

consentiva l'accesso all'elaboratore o nel caso di mancato utilizzo dei medesimi per un periodo superiore a sei mesi.

Modalità di difesa dai programmi pericolosi:

a) è vietato: al personale introdurre nel sistema floppy disk o cd rom di dubbia provenienza e/o non pertinenti al lavoro , scaricare da Internet programmi quali giochi, demo , software in genere non pertinente il lavoro ;
b) ogni pc è dotato di programmi Antivirus Norton e Ad-aware che vengono aggiornati automaticamente

Il sistema informatico non è connesso in alcun modo ad Internet.
Il sistema di back-up provvede a produrre ogni giorno una copia di sicurezza dell'intero sistema, le unità nastro vengono riposte in un luogo sicuro. Settimanalmente viene verificata la effettuava consistenza di tutto il sistema e dei back-up.

PUNTO IV

CRITERI E PROCEDURE PER LA SICUREZZA DELLE TRASMISSIONI DEI DATI, IVI COMPRESI QUELLI PER LE RESTRIZIONI DI ACCESSO PER VIA TELEMATICA.

Il sistema informatico non è connesso in alcun modo ad Internet.

PUNTO V

ELABORAZIONE DI UN PIANO DI FORMAZIONE PER RENDERE DOTTI GLI INCARICATI DEL TRATTAMENTO DEI RISCHI INDIVIDUATI E DEI MODI PER PREVENIRE I DANNI.

ANALISI DEI RISCHI E MODALITA' DI PREVENZIONE

RISCHIO – Accesso e/o sottrazione di Dati personali su supporto cartaceo

CONTROMISURE:

- I documenti cartacei vengono raccolti ordinatamente in cartelle non trasparenti e/o in schedari e, quando non utilizzati, riposti in apposite custodie munite di serratura.
- L'accesso di persone non autorizzate alle "aree ad accesso controllato" , dello studio e consentito solo se accompagnate da un addetto o sotto il controllo (anche solo visivo) di uno o più addetti.

- Le aree contenenti documentazione cartacea sono ubicate in modo tale che ciascun **incaricato** possa rilevare a vista il tentativo di accesso da parte di persone estranee ed impedirne l'accesso.
- È interdetto l'accesso alle “aree di accesso controllato” in orario diverso da quello di lavoro se non previa autorizzazione esplicita scritta e/o verbale da parte dei titolari.
- È vietato riprodurre documenti contenenti dati personali su scaffali in corridoi accessibili al pubblico.
- Al personale addetto vengono affidati i dati cartacei strettamente necessari ai compiti assegnati e viene verificata la restituzione delle pratiche al termine delle operazioni affidate.
- Nella copertina dei fax trasmessi è presente la seguente dicitura:

  (il contenuto di questo fax è riservato. Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo di telefax o di e-mail e distruggere il documento ricevuto erroneamente)

RISCHIO - accesso e/o sottrazione di dati personali su supporto Informatico:

CONTROMISURE:

- I floppy disk contenenti dati personali sono custoditi in contenitori con serratura ed una volta utilizzati vengono formattati.
- Ciascun addetto al trattamento è dotato di user-id e password per l'accesso al sistema informatico.
- Nelle sale con accesso consentito al pubblico non vengono mai lasciati accesi i computer se incustoditi.
- I fax e i server del sistema si trovano in aree ad accesso controllato o comunque non visibili al personale non addetto al trattamento dei dati ed al pubblico.
- È vietato consentire l’accesso al sistema a persone non espressamente autorizzate dai titolari

RISCHIO - Distruzione , danneggiamento del sistema informatico o interruzione totale o parziale del suo funzionamento da parte di programmi diretti a questo scopo - intromissione nel sistema informatico da parte di terzi non autorizzati al trattamento e alla custodia dei dati.

CONTROMISURE :

- L'amministratore del sistema deve impegnarsi periodicamente ad eseguire controlli sull'andamento degli strumenti di sicurezza e verifiche sulla preparazione del personale autorizzato all'utilizzo dei sistemi.
- Modalità di difesa dai programmi pericolosi:

a) è vietato al personale di introdurre floppy disk o cd rom di dubbia provenienza e/o non pertinenti al lavoro , scaricare da internet programmi quali giochi , demo , software in genere non pertinenti al lavoro ;

b) Ogni CD Rom o Floppy introdotto dal personale o dai tecnici esterni deve essere sempre controllato dal programma antivirus affinché sia certa l'assenza del virus.

c) Ogni PC è dotato di un programma antivirus che viene aggiornato con cadenza almeno mensile o più frequentemente se si rendono disponibili aggiornamenti da parte del fornitore.

d) Nel caso di utilizzo del sistema da parte di terzi (tecnici , consulenti) ridurre i rischi di intromissione consentendo l'accesso solo a persone fidate e di indubbia qualifica professionale al fine di evitare che vengano manomessi o asportati archivi o dati senza la previa autorizzazione dei titolari.

RISCHIO - Distruzione, danneggiamento o perdita di dati per malfunzionamento o guasti del sistema informatico o negligenza da parte del personale.

CONTROMISURE :

- Il back-up provvede ad effettuare una copia integrale di tutte le banche dati presenti in studio.
- Le copie vengono seguite ogni giorno su nastro magnetico e settimanalmente viene verificata l'integrità di tutto il sistema.
- L'incaricato materiale delle copie è Andrea Pulzetti o di un suo sostituto appositamente delegato in caso di sua temporanea impossibilità.
- Il funzionamento del sistema di back-up e del relativo ripristino viene verificato regolarmente.
- Il server è collegato ad un gruppo di continuità.

Gli incaricati del trattamento sono stati debitamente informati circa il contenuto del presente documento nel corso di una riunione, tenutasi in orario di lavoro, alla quale hanno partecipato i titolari e tutti gli incaricati al trattamento dei dati.