

**Documento programmatico sulla sicurezza dei dati ai sensi dell'articolo 35 D.Lgs. n. 196/2003
Nomina dei soggetti che effettuano il trattamento dei dati personali e sensibili**

AUTORIZZAZIONE PER MEDICI – COLLABORATORI

ARCHIVI CARTACEI

Il/La sottoscritto/a Dr./Dott.ssa

Cognome _____, Nome _____
Nato a _____, il _____ e Residente a _____
Via/P.zza _____, n° _____, con studio
medico in Via/P.zza _____, n° _____,
Città _____, Codice Regionale _____, MMG - PLG

Titolare del Trattamento dei dati ai sensi e per gli effetti dell'art.28 del D.Lgs. n. 196/2003, ai fini dell'applicazione della normativa vigente, adotta le seguenti disposizioni e dichiara che gli archivi cartacei relativi ai dati sanitari dei propri assistiti:

- Sono conservati presso lo studio in armadio munito di chiusura con chiave;
 Non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza e le persone che vi accedono sono pertanto preventivamente autorizzate.

Sono nominati "Incaricati del trattamento" art.30 D.Lgs. n. 196/2003 ed autorizzati:

- Cognome e Nome _____, Nato/a a _____, il __/__/____ con mansioni di Collaboratore di Studio.

Firma per Accettazione _____

- Cognome e Nome _____, Nato/a a _____, il __/__/____ con mansioni di Infermiere di Studio.

Firma per Accettazione _____

Agli incaricati sono state impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli incaricati del trattamento per lo svolgimento dei relativi compiti, sono stati avvertiti di controllare e custodire gli atti e documenti fino alla restituzione in maniera che ad esse non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

E' effettuato un aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative.

Sono previste procedure per un'ideale custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.

Sono previste procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità finalizzata all'identificazione degli incaricati.

I seguenti colleghi medici sono nominati “responsabili del trattamento” ed autorizzati ad accedere e trattare i dati personali dell’archivio delle cartelle cliniche dei propri assistiti, nei limiti delle necessità di diagnosi e cura degli stessi, nell’ambito di un rapporto di collaborazione, di sostituzione e secondo quanto previsto dagli accordi nazionali, regionale ed aziendale in tema di associazionismo:

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

Essi si atterrano scrupolosamente alle norme di legge e alle vigenti norme di deontologia medica.

Dopo l'orario di chiusura dello studio possono accedere ai locali i seguenti soggetti allo scopo di effettuare operazioni di pulizia e manutenzione:

1. Nome e Cognome: _____
Residente a _____ in via
_____, n° _____ con mansioni di pulizia.
2. Nome e Cognome: _____
Residente a _____ in via
_____, n° _____ con mansioni di manutenzione.

Tali soggetti non sono in possesso delle chiavi dell'armadio in cui sono conservati i dati su supporto cartaceo e non sono autorizzati ad accedere ai dati.

In fede.

Firma _____

Luogo e Data: _____ (___) ___/___/___/

**Documento programmatico sulla sicurezza dei dati ai sensi dell'articolo 35 D.Lgs. n. 196/2003
Nomina dei soggetti che effettuano il trattamento dei dati personali e sensibili**

AUTORIZZAZIONE PER MEDICI – COLLABORATORI

ARCHIVI ELETTRONICI

Il/La sottoscritto/a Dr./Dott.ssa

Cognome _____, Nome _____
Nato a _____, il _____ e Residente a _____
Via/P.zza _____, n° _____, con studio
medico in Via/P.zza _____, n° _____,
Città _____, Codice Regionale _____, MMG - PLG

Titolare del Trattamento dei dati ai sensi e per gli effetti dell'art.28 del D.Lgs. n. 196/2003, ai fini dell'applicazione della normativa vigente, adotta le seguenti disposizioni:

Sono nominati "Incaricati del trattamento" art.30 D.Lgs. n. 196/2003 ed autorizzati:

- Cognome e Nome _____, Nato/a a _____, il __/__/____/ con mansioni di Collaboratore di Studio.

Firma per Accettazione _____

- Cognome e Nome _____, Nato/a a _____, il __/__/____/ con mansioni di Infermiere di Studio.

Firma per Accettazione _____

- Cognome e Nome _____, Nato/a a _____, il __/__/____/ con mansioni di manutenzione informatica:

Hardware , Software , Rete , Amministratore di sistema .

Firma per Accettazione _____

Agli incaricati sono state impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli incaricati del trattamento per lo svolgimento dei relativi compiti, sono stati avvertiti di controllare e custodire gli atti e documenti fino alla restituzione in maniera che ad esse non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

E' effettuato un aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative.

Sono previste procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.

Sono previste procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità finalizzata all'identificazione degli incaricati.

Sono nominati “Responsabili del trattamento” art.29 D.Lgs. 196/2003

- Nessuno al di fuori del titolare. *Oppure*
- Cognome e nome _____, Nato/a il __/__/____/ a _____ con mansioni di _____
Firma per accettazione _____
- Cognome e Nome _____, Nato/a il __/__/____/ a _____ con mansioni di manutenzione informatica:
Hardware , Software , Rete , Amministratore di sistema .
- Firma per Accettazione _____

I seguenti colleghi medici sono nominati “Responsabili del trattamento” ed autorizzati ad accedere e trattare i dati personali dell’archivio delle cartelle cliniche dei propri assistiti, nei limiti delle necessità di diagnosi e cura degli stessi, nell’ambito di un rapporto di collaborazione, di sostituzione e secondo quanto previsto dagli accordi nazionali, regionale ed aziendale in tema di associazionismo:

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all’Ordine dei Medici di _____
Firma per accettazione _____

- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all'Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all'Ordine dei Medici di _____
Firma per accettazione _____
- Il/La Dott./ssa _____, medico sostituto associato
residente a _____, via _____,
n° _____, iscritto all'Ordine dei Medici di _____
Firma per accettazione _____

Essi si atterrano scrupolosamente alle norme di legge e alle vigenti norme di deontologia medica.

Dopo l'orario di chiusura dello studio possono accedere ai locali i seguenti soggetti allo scopo di effettuare operazioni di pulizia e manutenzione:

Nome e Cognome: _____
Residente a _____ in via _____,
n° _____ con mansioni di pulizia.

Nome e Cognome: _____
Residente a _____ in via _____,
n° _____ con mansioni di manutenzione.

Tali soggetti non sono in possesso delle chiavi dell'armadio in cui sono conservati i dati su supporto cartaceo, non sono dotati di alcuna password e non sono autorizzati ad accedere ai dati.

In fede.

Firma _____

Luogo e Data: _____ (___) ___/___/___/

**Documento Programmatico sulla Sicurezza (DPS) dei dati ai sensi del
D.Lgs. n. 196/2003, artt.31-36 ed allegato tecnico (B)**

**TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON
STRUMENTI ELETTRONICI**

Il/La sottoscritto/a Dr./Dott.ssa

Cognome _____, Nome _____
Nato a _____, il _____ e Residente a _____
Via/P.zza _____, n° _____, con studio medico in
Via/P.zza _____, n° _____,
Città _____, Codice Regionale _____, MMG - PLG

DICHIARA

1. **di svolgere la propria attività di Medicina Generale Pediatra di Libera Scelta convenzionata avvalendosi dello strumento informatico per la tenuta delle schede sanitarie individuali** (previste come obbligo contrattuale dal vigente Accordo Collettivo Nazionale).
2. **di essere l'unico Titolare del Trattamento dei dati**
3. **di** **non utilizzare personale di studio e/o infermieristico**
 utilizzare: collaboratore di studio ; personale infermieristico
4. **di aver avviato il seguente programma di adeguamento alle misure di sicurezza previste ai sensi D.Lgs. n. 196/2003, artt.31-36 ed allegato tecnico (B) rispetto agli archivi magnetici**, contenuti sul/sui computer che si trova/trovano nello/negli studio/i sottoelencato/i al fine di garantire sia la non accessibilità da parte di soggetti non autorizzati sia l'integrità fisica:
 1° studio: Via/Piazza _____, n° _____, _____ (____)
 Altri studi: Via/Piazza _____, n° _____, _____ (____)
Via/Piazza _____, n° _____, _____ (____)
 e/o su PC portatile
5. **di aver compilato questo DPS sulla sicurezza dei dati sensibili entro il __/__/____/**, scadenzando entro il 31 marzo di ogni anno il termine per il suo aggiornamento.
6. **di aver predisposto l'elenco dei trattamenti in atto o possibili:**
 Dati personali degli assistiti e personali di fornitori e/o clienti.
 Dati personali del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria.
 Dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria.
 Dati personali di Avvocati e professionisti cui vengono affidati incarichi o cui ci si rivolge per consulenze nonché inerenti a finalità fiscali o dati di natura bancaria;
 Dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente o l'adesione ad organizzazioni sindacali;
 Dati sensibili degli assistiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;
 Dati sensibili dei paziente, dagli stessi forniti o comunque acquisiti per l'espletamento idonei a rivelare lo stato di salute;
 Dati sensibili di terzi, forniti dai pazienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;
 Dati sensibili di clienti o terzi, comunque afferenti la vita sessuale.

7. di aver predisposto nell'ambito dei dati personali degli assistiti:

- L'elenco dei trattamenti di dati personali (regola 19.1.):

Raccolta ; Registrazione ; Aggiornamento ; Conservazione ; Modificazione ; Comunicazione ; Cancellazione ; Blocco .

- Le informazioni di base e descrizione degli strumenti utilizzati:

Attività di MMG PLS convenzionato: singolo; associato; in rete; di gruppo

Finalità perseguite: diagnosi e cura; ricerca e statistica

Struttura di riferimento: studio/i medici come sopra riportato/i

Descrizione degli strumenti elettronici utilizzati: Pc utilizzato: fisso, portatile

non collegato ad Internet; collegato in rete: locale, geografica, Internet, VPN

L'archivio delle cartelle cliniche è memorizzato:

in un HD non rimovibile;

in un HD rimovibile che si può inserire con una chiave in possesso solo del titolare del trattamento dei dati;

8. di aver provveduto alla seguente distribuzione dei compiti e delle responsabilità nell'ambito delle figure preposte al trattamento dei dati personali (regola 19.2.) redigendo specifici documenti:

a. Responsabili del trattamento:

Titolare: Dr. Responsabile unico

Sono stati nominati "altri responsabili del trattamento", art.29 D.Lgs. 196/2003 secondo apposito documento (Medici sostituti: ; MMG/PLS in associazione o rete o gruppo ; amministratore di rete e/o di sistema);

b. Incaricati del trattamento, art.30 D.Lgs. 196/2003, nominati ed autorizzati secondo apposito documento con specifiche passwords e profili di autorizzazione, specifici o per classi omogenee di incaricati, individuati e configurati anteriormente all'inizio del trattamento:

Collaboratore di studio con mansioni di segreteria; Infermiere

A ciascuno dei Responsabili e degli Incaricati è stato dato:

un codice identificativo (ID-user name) associato ad una parola chiave riservata (Password-PW) per l'avvio del sistema operativo Windows conosciute solamente dal medesimo.

oppure una smart card o altro dispositivo o dato biometrico d'autenticazione eventualmente associato ad un codice identificativo o ad una parola chiave, ad uso esclusivo del singolo incaricato, per l'accesso dei dati da trattare.

un codice identificativo utente ID e da una password PW per l'avvio del programma che gestisce l'archivio delle cartelle cliniche degli assistiti conosciute solo dal medesimo, con livello di accesso assegnato dal titolare.

A ciascuno dei Responsabili e degli Incaricati è stato prescritto:

di adottare le necessarie cautele per assicurare la segretezza della password, la diligente custodia dei dispositivi d'accesso ad uso esclusivo dell'incaricato;

che la password sia composta da almeno otto caratteri o altrimenti da un numero di caratteri pari al massimo consentito dal programma gestionale utilizzata;

di verificare che la password non contenga riferimenti agevolmente riconducibili all'incaricato;

di provvedere a modificare la password al primo utilizzo e, successivamente, almeno ogni tre mesi, se tratta dati personali sensibili (tipo quelli dei MMG-PLS), o almeno ogni sei mesi se tratta altri dati.

Per ciascuno dei Responsabili e degli Incaricati è stato verificato che:

il codice identificativo, ove utilizzato, non sia assegnato ad altri Incaricati, neppure in tempi diversi;

codici, parole chiave e dispositivi d'autenticazione non utilizzati da almeno sei mesi debbano essere disattivati, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

codici identificativi, passwords e dispositivi d'autenticazione per l'accesso ai dati siano disattivati nel caso in cui all'Incaricato non sia più consentito l'accesso ai dati personali;

la custodia delle copie delle credenziali in modo sia organizzata in modo da garantire la relativa segretezza e siano stati individuati preventivamente per iscritto gli incaricati della loro custodia.

A ciascuno dei Responsabili e degli Incaricati è stato impartito:

- di non lasciare incustodito e accessibile il PC, il notebook, il palmare o altra postazione elettronica durante una sessione di lavoro e di chiudere accuratamente armadi, schedari e computer al termine del proprio lavoro;
- disposizioni scritte sulle modalità d'accesso alla postazione di lavoro e a dati in casi di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità d'operatività e di sicurezza del sistema;
- di informare tempestivamente l'Incaricato dell'intervento effettuato;
- una istruzione organizzativa e tecnica per la custodia e l'uso di floppy disk, cd-rom o altri supporti rimovibili sui quali contenenti dati sensibili se non utilizzati al fine di evitare accessi non autorizzati o trattamenti non consentiti.

9. di aver adottato i seguenti sistemi di aggiornamento periodico dell'autorizzazione di accesso e trattamento:

- un sistema di autorizzazione per disciplinare diversi ambiti individuali di trattamento consentito e modalità di accesso degli Incaricati (Collaboratori, Sostituti, ect.)
- profili d'autorizzazione in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento (per classi omogenee di incaricati od anche con riferimento al singolo Incaricato);
- verifica periodica, almeno una volta l'anno, della lista degli Incaricati e che persistano i presupposti per il profilo d'autorizzazione di ciascun Incaricato;
- verifica periodica, e comunque almeno una volta l'anno, dell'ambito di trattamento di dati personali consentito agli addetti alla gestione e/o alla manutenzione dei sistemi informativi, hardware, software e database.

10. di aver attuato la protezione degli strumenti elettronici e dei dati mediante analisi dei rischi che incombono sui dati (regola 19.3) ed adozione di misure per contrastare i rischi individuali (regola 19.4) e per la protezione delle aree e dei locali rilevanti ai fini della custodia e dell'accessibilità ai dati.

Elenco dei principali eventi potenzialmente dannosi per la sicurezza dei dati, delle possibili conseguenze e della gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati, con impatto prevedibile sulla sicurezza ed eventuali provvedimenti adottati o da adottare:

- a. *Comportamento degli operatori* (impatto sulla sicurezza=rilevanza e probabilità medio bassa).
 - le credenziali di autenticazione non possono essere sottratte da terzi in quanto note solo agli operatori.
 - copia delle credenziali è nascosta in armadio (a muro) sempre chiuso a chiave non in possesso di terzi.
- b. *Eventi relativi agli strumenti* (impatto sulla sicurezza=rilevanza e probabilità medio bassa).
 - programmato almeno ogni sei mesi, se si tratta dati sensibili, o altrimenti almeno ogni anno, l'aggiornamento periodico dei softwares con ricezione anche di patches per prevenire la vulnerabilità dei sistemi informativi e correggerne i difetti:
 - Sistema operativo in uso (quelli che garantiscono effettivamente di attivare credenziali di autenticazione es. Windows 2000, Mac OS X, Linux):
 - Installazione software in grado di prevenire vulnerabilità e/o correggere difetti degli strumenti elettronici: es. Patch di windows.
 - predisposto idonei dispositivi e programmi elettronici per la protezione dei dati dal rischio di intrusione e dall'azione di software volti a danneggiare e/o interrompere il funzionamento dei sistemi informatici (azione di virus informatici o di programmi suscettibili di recare danno spamming o tecniche di sabotaggio):
 - il computer è dotato di firewall:
 - il programma antivirus è:
 - predisposto aggiornamento dei dispositivi anti-intrusione e antivirus:
 - costante ed automatico ad ogni collegamento; almeno ogni sei mesi, con ricambio manuale.

- c. *Malfunzionamento, indisponibilità o degrado degli strumenti* (impatto sulla sicurezza=rilevanza e probabilità medio bassa).
 le copie di backup dei dati sono effettuate al massimo settimanalmente.
 le copie di backup sono salvate su CD custodito in armadio (a muro) sempre chiuso a chiave non in possesso di terzi non autorizzati.
 un secondo computer nello studio, non collegato ad Internet ha il programma gestionale montato senza dati e predisposto per poter funzionare con i dati di backup.
- d. *Accessi esterni non autorizzati – Intercettazione di informazioni in rete* (impatto sulla sicurezza=rilevanza e probabilità medio bassa).
 computer contenente il data base gestionale scollegato da Internet.
 mai collegato ad Internet durante l'utilizzo del programma gestionale.
 collegamento in rete tramite VPN.
 utilizzo di idonei strumenti di protezione dei dati sensibili contro l'accesso abusivo:
 firewall, Antivirus.
 utilizzo del programma: prodotto dalla società e distribuito da Il programma è dotato e protetto da password individuali di accesso.
- e. *Eventi relativi al contesto fisico-ambientale* (impatto sulla sicurezza=rilevanza e probabilità medio bassa).
- Ingressi non autorizzati a locali/aree ad accesso ristretto:
 Ubicazione dello studio: primo piano, Altro piano (specificare):
 Protezioni: sistema d'allarme.
 porte blindate d'accesso sala attesa e sala studio.
 porta di separazione sala attesa-studio chiusa a chiave al termine dell'orario con indicazione in tal senso sia ai sostituti che agli addetti alle pulizie.
 accesso allo studio: possibile per gli utenti solo in presenza del medico o del collaboratore di studio
- Sottrazione di strumenti contenenti dati (accessibilità ai dati in assenza del medico):
 cartelle cliniche cartacee: chiuse in un armadio (a muro) chiuso a chiave, con chiave inaccessibile a terzi.
 referti – ricette in studio: poste in buste chiuse in cassetto e con chiave inaccessibile a terzi non autorizzati.
 modalità consegna – rinnovo ricette – proposte:
 la consegna avviene da parte degli utenti in cassetta/e di tipo postale tali da non poter estrarre i documenti introdotti, posta/e all'interno della sala d'attesa e/o di fianco all'entrata della sala d'attesa.
 riconsegna: avviene direttamente al paziente od al suo delegato specificatamente dallo stesso autorizzato.
 personale addetto alle pulizie: non in possesso di codici o password di accesso al computer né di chiave per armadi e/o cassette con notizie degli utenti.
- f) *Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria* (impatto sulla sicurezza=rilevanza e probabilità medio bassa):
Le copie di backup sono in:
 armadio a muro; altro tipo di armadio.
 in custodia anti-urto ed anti-perturbazioni elettromagnetiche.
 uno studio dotato di sistema: antiallagamento con scolo d'acqua; antincendio.
- g) *Guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)* (impatto sulla sicurezza=rilevanza e probabilità medio bassa):
Lo studio è dotato di: impianti elettrici e di riscaldamento a norma con manutenzione
 climatizzatore luci di emergenza gruppi di continuità

h) *Errori umani nella gestione della sicurezza fisica* (impatto sulla sicurezza=rilevanza e probabilità medio bassa):

il computer ed il gruppo di continuità sono posti in sedi non soggetti ad urti o possibilità di danneggiamento con liquidi da parte del personale di servizio.

Tutte le misure sopra riportate sono già in essere.

Eventuali misure da adottare (indicare i tempi previsti per la sua messa in opera):

per ora nessuna; oppure

11. di aver predisposto criteri e modalità di salvataggio e di ripristino della disponibilità dei dati in caso di loro danneggiamento o di inaffidabilità della base dei dati o degli strumenti elettronici (regola 19.5) (disaster recovery):

a) Banca dati/Data base/Archivio:

Banca dati (anche più di una): Proprio computer; Server di Gruppo; Server di rete VPN;

Altro (Specificare):

Data base utilizzato: Phronesis Millenium; Profim; Perseo; Altro ::.....

b) Criteri e procedure per il salvataggio e il ripristino dei dati:

I dati vengono salvati ogni sette giorni al massimo, mediante scrittura con apposito programma, su:

CD ROM Hard Disk secondario

Dispositivo Iomega ZIP Chiave USB

Altro dispositivo (specificare):

In caso di danneggiamento dei dati o degli strumenti elettronici, il ripristino, in tempi certi compatibili con i diritti degli interessati, può avvenire immediatamente per i dati, con tecnica semplice di copia incolla ed in tempo non superiore a sette giorni per i danni agli strumenti elettronici.

c) Pianificazione delle prove di ripristino:

Il tempo previsto per effettuare i tests di efficacia delle procedure di salvataggio/ripristino dei dati adottate è molto breve, dell'ordine di 5-10 minuti massimo.

d) Modalità di custodia delle copie:

Il luogo fisico in cui sono custodite le copie di backup dei dati salvate è:

un armadio a muro entro il perimetro dello stesso studio chiuso con chiave inaccessibile a terzi non autorizzati.

un armadio metallico fissato a muro entro il perimetro dello studio chiuso con chiave inaccessibile a terzi non autorizzati.

Altro (specificare):

e) Struttura o persona incaricata del salvataggio:

La persona incaricata di effettuare il salvataggio e/o di controllare l'esito:

è il Titolare dello studio: dr.

Altro nominato ed autorizzato con apposito documento (specificare):

12. di aver pianificato gli interventi formativi previsti (regola 19.6):

Titolare: Il titolare ha partecipato e partecipa a corsi di formazione sulla privacy, riceve notizie in merito direttamente dal proprio Sindacato di categoria FIMMG e consulta periodicamente il sito WEB del garante per la Protezione dei Dati personali. Il tempo medio degli eventi formativi è di quattro ore ogni sei mesi in aula e di quindici minuti al mese sul sito web.

Incaricati: previsti interventi formativi per renderli edotti:

a. dei rischi che incombono sui dati;

b. delle misure disponibili per prevenire eventi dannosi;

c. dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;

d. delle responsabilità che ne derivano;

e. delle modalità per aggiornarsi sulle misure minime adottate dal titolare;

programmata la formazione di ciascun incaricato al momento dell'ingresso in servizio.

programmati momenti formativi ed addestrativi di durata adeguata verso ciascun incaricato in occasione di cambiamenti di mansioni o di introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc., rilevanti rispetto al trattamento di dati personali.

13. di aver predisposto le misure necessarie per trattamenti affidati all'esterno (regola 19.7):

- Attualmente non sono affidati trattamenti all'esterno.
- In caso di esternalizzazione del trattamento, è stato redatto un apposito quadro sintetico delle attività affidate a terzi che comportano il trattamento dei dati con indicazione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza.

(Descrizione dell'attività esternalizzata; Trattamenti di dati interessati sensibili effettuati nell'ambito della predetta attività; Indicazione della società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina Sulla protezione dei dati personali (titolare o responsabile del trattamento); Descrizione scritta dell'intervento effettuato ed attestazione della sua conformità alle disposizioni del Disciplinare Tecnico previsto dal Codice sulla Privacy; Descrizione dei criteri che garantiscono un adeguato trattamento, con particolare riferimento, ad esempio, a:

1. Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. Adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
3. Rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. Impegno a relazionare periodicamente sulle misure di sicurezza adottate, anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze).

- Programmato di riferire nella relazione accompagnatoria del bilancio di esercizio della eventuale propria società di servizio di supporto al proprio associazionismo, l'avvenuta redazione del Documento Programmatico sulla Sicurezza.

14. di aver adottato criteri per cifrare o separare dai dati i dati identificativi idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari ed esercenti le professioni sanitarie (regole 19.8 e 24) in caso di particolari forme di elaborazione:

- Interconnessione, raffronti, incroci di dati con altri soggetti pubblici o privati (specificare quali ed indicarne i motivi), (es. sistemi informativi regionali : specificare chi è il titolare dei dati del sistema):

.....
.....
.....
.....

- Altre operazioni: (indicare altre eventuali operazioni effettuate sui dati in questione diverse da quelle enunciate precedentemente)

.....
.....
.....

In fede, Firma

Luogo e data:(.....) ____/____/____

MONITORAGGIO DEL PROCESSO DI TRATTAMENTO

In occasione della revisione del documento programmatico della sicurezza, che dovrà essere effettuato entro il di ogni anno, andranno verificate le seguenti circostanze e programmati gli interventi correttivi in relazione al progresso della tecnica ed ai rischi emersi nel corso dell'anno che in sede di prima analisi si è così valutato:

(Misura richiesta SOLUZIONE ADOTTATA O DA ADOTTARE)

1. Censimento e aggiornamento dei trattamenti: Adottato; Da adottare
2. Lista degli incaricati: Adottato; Da adottare
3. Gestione delle credenziali di autenticazione: Adottato; Da adottare
4. Password, token o dispositivi biometrici (togliere quello che non è stato adottato): Adottato; Da adottare
5. Protezione della sessione di lavoro: Adottato; Da adottare
6. Profilazione dei privilegi per l'accesso: Adottato; Da adottare
7. Aggiornamento programmi per prevenire vulnerabilità e correggere difetti del software: Adottato; Da adottare
8. Adozione di misure idonee per assicurare l'integrità e disponibilità dei dati:
 Adottato; Da adottare
9. Salvataggio e ripristino dati: Adottato; Da adottare
10. Disaster recovery (COSIGLIABILE MA NON OBBLIGATORIO) : Adottato;
 Da adottare
11. Ripristino dei dati e sistemi salvati: Adottato; Da adottare Adottato
12. Difesa dagli accessi abusivi: Adottato; Da adottare
13. Protezione supporti rimovibili: Adottato; Da adottare
14. Analisi dei rischi informatici: Adottato; Da adottare
15. Relazione di conformità dell'installatore per adozione misure minime:
 Adottato; Da adottare
16. Formazione specifica degli incaricati: **PREVISTA DA ADOTTARE**

Autorizzazione e disposizioni scritte per i Responsabili e per gli Incaricati del trattamento

Il/La sottoscritto/a Dr./Dott.ssa

Cognome _____, Nome _____
Nato a _____, il _____ e Residente a _____
Via/P.zza _____, n° _____, con studio medico in
Via/P.zza _____, n° _____,
Città _____, Codice Regionale _____, MMG - PLG

Titolare del Trattamento dei dati ai sensi e per gli effetti dell'art.28 del D.Lgs. n. 196/2003, ai fini dell'applicazione della normativa vigente, adotta le seguenti disposizioni:

E' nominato "Responsabile del trattamento" art.29 D.Lgs. 196/2003

Nessuno al di fuori del titolare. *Oppure*

Cognome e nome _____, Nato/a il ___/___/___/ a
_____ Firma per accettazione _____

nelle vesti di Sostituto; MMG/PLS in associazione o rete o gruppo; Amministratore di rete/sistema.

E' nominato "Incaricato del trattamento" art.30 D.Lgs. n. 196/2003 ed autorizzato:

Cognome e nome _____, Nato/a il ___/___/___/ a
_____ Firma per accettazione _____

nelle vesti di Collaboratore di studio con mansioni di segreteria; Infermiere ; Informatico con mansioni di assistenza all'hardware e/o al software

* Al suddetto **Responsabile o Incaricato è stato dato:**

- un codice identificativo (ID-user name) associato ad una parola chiave riservata (Password-PW) per l'avvio del sistema operativo Windows conosciute solamente dal medesimo.
- oppure una smart card o altro dispositivo o dato biometrico d'autenticazione eventualmente associato ad un codice identificativo o ad una parola chiave, ad uso esclusivo del singolo incaricato, per l'accesso dei dati da trattare.
- un codice identificativo utente ID (.....) e da una password PW (.....) per l'avvio del programma che gestisce l'archivio delle cartelle cliniche degli assistiti conosciute solo dal medesimo, con livello di accesso assegnato dal titolare.

* Al suddetto **Responsabile o Incaricato è stato prescritto:**

- di adottare le necessarie cautele per assicurare la segretezza della password, la diligente custodia dei dispositivi d'accesso ad uso esclusivo dell'incaricato;
- che la password sia composta da almeno otto caratteri o altrimenti da un numero di caratteri pari al massimo consentito dal programma gestionale utilizzata;
- di verificare che la password non contenga riferimenti agevolmente riconducibili all'incaricato;
- di provvedere a modificare la password al primo utilizzo e, successivamente, almeno ogni tre mesi, se tratta dati personali sensibili (tipo quelli dei MMG-PLS), o almeno ogni sei mesi se tratta altri dati.

* Col suddetto **Responsabile o Incaricato è stato verificato che:**

- il codice identificativo, ove utilizzato, non sia assegnato ad altri Incaricati, neppure in tempi diversi;
- codici, parole chiave e dispositivi d'autenticazione non utilizzati da almeno sei mesi debbano essere disattivati, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- codici identificativi, passwords e dispositivi d'autenticazione per l'accesso ai dati saranno disattivati nel caso in cui all'Incaricato non sia più consentito l'accesso ai dati personali;
- Copie delle credenziali saranno custodite in:
 - un armadio a muro entro il perimetro dello stesso studio chiuso con chiave inaccessibile a terzi non autorizzati.
 - un armadio metallico fissato a muro entro il perimetro dello studio chiuso con chiave inaccessibile a terzi non autorizzati.
 - Altro (specificare):

* Al suddetto **Responsabile o Incaricato è stato impartito:**

- di non lasciare incustodito e accessibile il PC, il notebook, il palmare o altra postazione elettronica durante una sessione di lavoro e di chiudere accuratamente armadi, schedari e computer al termine del proprio lavoro;
- disposizioni sulle modalità d'accesso alla postazione di lavoro e a dati in casi di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità d'operatività e di sicurezza del sistema;
- di informare tempestivamente l'Incaricato dell'intervento effettuato;
- una istruzione organizzativa e tecnica per la custodia e l'uso di floppy disk, cd-rom o altri supporti rimovibili sui quali contenenti dati sensibili se non utilizzati al fine di evitare accessi non autorizzati o trattamenti non consentiti.

Luogo e data: (.....) ___/___/_____

Letto e firmato

Il titolare

Il responsabile

L'incaricato

MODULO CONSENSO INFORMATO
(D.Lgs 196/2003)

Io sottoscritto :

Nato a, il

Residente a

Assistito del dr.e dallo stesso informato su:

1. la necessità di raccogliere i dati personali, anagrafici riferiti alle mie condizioni di salute;
2. il fatto che tali informazioni verranno trattate con strumenti elettronici per finalità connesse alle attività di prevenzione, diagnosi, cura e riabilitazione a tutela della mia salute;
3. il trattamento dei dati personali per scopi scientifici (ricerca scientifica e/o sperimentazione clinica controllata di medicinali), nell'ambito della teleassistenza o telemedicina, per fornire altri beni e servizi attraverso una rete di comunicazione elettronica;
4. la possibilità che tali informazioni potranno essere fornite in forma anonima a terzi per effettuare ricerche epidemiologiche ed analisi statistiche; tali informazioni potranno essere rielaborate, in forma aggregata e anonima e quindi senza nessun riferimento alle persone.
Sempre per queste finalità i dati potranno essere comunicati anche a soggetti che forniscono servizi di analisi in laboratorio e che permettono l'aggiornamento e l'informazione medico-scientifica, precisando che tali informazioni non saranno in ogni caso cedute a terzi;
5. la possibilità che i dati informatici in suo possesso verranno trattati da terzi per la sincronizzazione degli stessi da/verso un unico Data Center per rendere possibile l'interscambio della cartella con i colleghi della medicina in rete, durante la visita ambulatoriale;
6. le misure atte a garantire la riservatezza delle informazioni;

ESPRIMO IL MIO CONSENSO E AUTORIZZO

Il dr. i medici sostituiti e in associazione
....., nonché eventuali collaboratori da lui autorizzati.

Tale consenso è esteso anche a gruppi di cura esterni (Specialisti, reparti ospedalieri, Emergenza) attivati dal dr.

.....

FIRMA

Li,

.....

Letta l'informativa nego il mio consenso per:

* tutto quanto in premessa:

* solo per i seguenti punti:

FIRMA

.....

**MODULO CONSENSO INFORMATO MINORI
(D.Lgs 196/2003)**

Io sottoscritto :

Nato il a, Residente a

In qualità di esercente la patria potestà del minore

Nato il assistito del dr.

e dallo stesso informato su:

1. la necessità di raccogliere i dati personali, anagrafici riferiti alle condizioni di salute;
2. il fatto che tali informazioni verranno trattate con strumenti elettronici per finalità connesse alle attività di prevenzione, diagnosi, cura e riabilitazione a tutela della salute del minore;
3. il trattamento dei dati personali per scopi scientifici (ricerca scientifica e/o sperimentazione clinica controllata di medicinali), nell'ambito della teleassistenza o telemedicina, per fornire altri beni e servizi attraverso una rete di comunicazione elettronica;
4. la possibilità che tali informazioni potranno essere fornite in forma anonima a terzi per effettuare ricerche epidemiologiche ed analisi statistiche; tali informazioni potranno essere rielaborate, in forma aggregata e anonima e quindi senza nessun riferimento alle persone.
Sempre per queste finalità i dati potranno essere comunicati anche a soggetti che forniscono servizi di analisi in laboratorio e che permettono l'aggiornamento e l'informazione medico-scientifica, precisando che tali informazioni non saranno in ogni caso cedute a terzi;
5. la possibilità che i dati informatici in suo possesso verranno trattati da terzi per la sincronizzazione degli stessi da/verso un unico Data Center per rendere possibile l'interscambio della cartella con i colleghi della medicina in rete, durante la visita ambulatoriale;
6. le misure atte a garantire la riservatezza delle informazioni;

ESPRIMO IL MIO CONSENSO E AUTORIZZO

Il dr. i medici sostituti e in associazione
....., nonché eventuali collaboratori da lui autorizzati.

Tale consenso è esteso anche a gruppi di cura esterni (Specialisti, reparti ospedalieri, Emergenza) attivati dal dr.

.....

FIRMA

Lì,

.....

Letta l'informativa nego il mio consenso per:

* tutto quanto in premessa:

* solo per i seguenti punti:

FIRMA

.....