DISCLAIMER

La presente documentazione costituisce una base su cui definire le procedure che vanno personalizzate considerando le singole esigenze dello Studio.

La presente documentazione non è utilizzabile in tutti i casi di possibile interesse ma va personalizzata secondo le diverse tipologie organizzative.

Non si assume alcuna responsabilità per l'uso della presente documentazione.

Regolamento UE 679/2016 in materia di privacy e data protection.
Valutazione di impatto sul trattamento dei dati
Risk assessment

Il trattamento dei dati personali / sensibili all'interno dello Studio Medico Pediatrico avviene con l'utilizzo prevalente di strumenti informatici attraverso programmi specialistici che comportano la presenza dei dati stessi su cloud (gestito all'interno dell'Unione Europea) e/o anche su sistema locale. I programmi specialistici sono preventivamente "verificati" dagli enti territoriali di riferimento con i quali scambiano dati per esempio per la gestione della Cartella Sanitaria del Paziente. I dati personali sono trattati per le finalità istituzionali espresse in dettaglio nelle Informative fornite preventivamente ad ogni Paziente.

I dati saranno trattati dal Titolare, dai Responsabili e dagli Incaricati preposti, nonché dal personale paramedico e di segreteria compresi i Medici chiamati in sostituzione ovvero i professionisti operanti in associazione o in medicina di gruppo o di rete. Tali dati saranno trattati solo nei limiti strettamente necessari allo svolgimento dei Loro compiti, avendone cura di proteggere la riservatezza, nel rispetto delle norme vigenti. Ogni incaricato/responsabile è preventivamente istruito e usa proprie credenziali di autorizzazione/autenticazione.

Valutazione preventiva delle misure di sicurezza (*barrare le caselle di interesse*).

□ Il trattamento effettuato dei dati personali è necessario e proporzionale e fatto per le sole attività istituzionali di medicina e assistenza sanitaria del Paziente, e per le attività, espressamente indicate in informativa, inerenti la ricerca scientifica e lo scambio di informazioni con il Servizio Sanitario Nazionale ed altri Enti Istituzionali.

□ accesso ai locali ove avviene il trattamento dai dati:
- □ protetto da sistema di allarme antiintrusione
- □ vigilanza con intervento in loco in breve tempo per la messa in sicurezza dei locali
- □ dotato di sistema di videosorveglianza
- □ dotato di inferriate di sicurezza

□ gestione informatica dei dati con le seguenti misure di sicurezza:
- □ accesso protetto la login e password personale di complessità adeguata e variata Periodicamente;
- □ sistema informatico protetto, se connesso in rete, da firewall opportunamente aggiornato;
- □ sistema antivirus opportunamente aggiornato
- □ sistemi operativi adeguati e aggiornati e programmi applicativi opportunamente aggiornati
- □ sistema di backup completo dei dati personali con conservazione dei supporti in

Locali diversi da quelli ove è presente il sistema informatico
□ cifratura della base dati.
□ backup protetto da password di accesso e/o crittografia dei dati
□ procedura di recupero dei dati con verifica periodica
□ durante una sessione di trattamento di dati il sistema non è mai lasciato incustodito

□ dichiarazione di conformità del software utilizzato per la gestione dei dati personali al Regolamento UE 216/679.

□ gestione della base dati con indirizzamento anonimo in modo da non avere un Collegamento diretto tra dati e interessati.

□ verifica periodica dei sistemi antiintrusione con controllo periodico dei registri di accesso per monitorare e prevenire seri tentativi di intrusione attraverso la rete informatica.

□ Formazione specifica ai Lavoratori interni in merito ai principi fondamentali e alle procedure in essere.

□ gestione cartacea dei dati con le seguenti misure di sicurezza:
□ conservazione in armadio di sicurezza chiuso e ad accesso controllato e riservato

□ procedura per segnalazione all'autorità di controllo competente, entro 72 ore dal momento in cui si ha notizia, una violazione di dati personali.

□ La gestione dei dati personali permette l'agevole salvaguardia dei diritti e della libertà degli interessati.

□ La gestione dei dati personali con le procedure tecniche e organizzative implementate permette di ritenere trascurabile il rischio di accesso abusivo ai dati e di violazione della privacy ma anche di distruzione o alterazione abusiva delle informazioni.

□ La presente valutazione dei rischi consente di ritenere la gestione dei dati personali adeguata alle necessità con misure di sicurezza idonee allo scopo, al rischio e alle finalità perseguite.

□ Ogni variazione al contesto operativo viene preventivamente analizzata per accertare se le misure di sicurezza in essere sono ancora idonee e sufficienti.

□ I dati personali gestiti anche da Medici sostituti, in Associazione, Medici in gruppo e personale amministrativo avvengono sulla base di nomine quali Responsabili o Incaricati del Trattamento ed è stato preventivamente verificata la loro competenza e organizzazione nella gestione e nel rispetto delle misure di sicurezza.

Si indica altresì il seguente percorso di miglioramento, da attuare entro il ……..

□ una valutazione di impatto sul trattamento dei dati per i software utilizzati, attraverso richiesta esplicita ai produttori anche in merito alla conservazione dei dati stessi su sistemi cloud, alla gestione operativa di un'eventuale richiesta di "oblio" , "portabilità dei dati", "accesso", " limitazione del trattamento" e alle procedura di sicurezza in genere per attestarne la conformità alla normativa vigente.

□ una revisione dei sistema informativo in particolare in relazione alla necessità di continuo aggiornamento dei sistemi di protezione (antivirus, firewall, sistemi operativi, anti intrusione, backup,…….) con personale tecnico specializzato, qualora non presente internamente allo Studio Medico.

□ eliminazione trattamento cartaceo dai dati personali (escluso obblighi di legge)

□ formazione periodica dei Responsabili e degli Incaricati in merito alla normativa vigente in materia di protezione dei dati personali e gestione del rischio associata

□
……

□
……

□
……

□
……

Data, ……..

Il Titolare del Trattamento

……..