F.I.M.P.
Federazione Italiana Medici Pediatri
Regione Veneto

Regolamento Privacy UE 679/2016
notizie utili per il Pediatra

In Italia la prima legge in materia di trattamento dei dati personali risale al 1996 legge 675, sostituita in seguito dal D.lgs. n° 196/2003, dal 25 maggio 2018 entra in vigore il nuovo Regolamento europeo n° 679/2016 che non richiede una legge di recepimento nazionale ed è direttamente applicabile.

Il nuovo regolamento amplia e rafforza la tutela delle persone fisiche, introduce nuovi obblighi, stabilisce criteri rigorosi per i casi di violazione dei dati (data breach) e inasprisce le sanzioni.

Il regolamento introduce la nuova figura del **DPO (Data Protection Officer)** che dovrà consigliare ed informare il titolare o il responsabile del trattamento e verificare l'applicazione delle norme. Tale figura si applica ai soggetti che trattano dati sensibili su "larga scala" es grandi strutture sanitarie.

Titolare del trattamento: nel caso dello studio medico è il pediatra stesso, cioè la persona fisica cui compete le scelte di fondo sulle finalità e sulle modalità di trattamento dei dati, anche per ciò che riguarda la sicurezza.

Responsabile del trattamento: è la persona fisica che tratta dati personali per conto del titolare del trattamento. Nel caso del Pediatra la figura del titolare del trattamento dei dati coincide anche con quella del responsabile.

Incaricato del trattamento dei dati: è la persona fisica autorizzata a compiere le operazioni di trattamento dal titolare o dal responsabile tramite sottoscrizione firmata di incarico. Nel caso dello studio medico ad esempio la collaboratrice di studio, il medico sostituto, i pediatri in associazione/gruppo/rete.

Il pediatra deve ottemperare alle norme sulla privacy innanzitutto fornendo una corretta **informativa** sul trattamento dei dati personali in forma proattiva.

Informativa: è una dichiarazione scritta con la quale si informa i pazienti su quali dati verranno raccolti per un efficace rapporto medico/paziente e chi, oltre al medico, ne verrà a conoscenza. L'informativa può essere consegnata al paziente o affissa nella sala d'attesa dello studio in **modo bene visibile.**

Raccolta del consenso : dopo aver informato il paziente il Pediatra deve raccogliere il consenso con la sottoscrizione di un modulo all'inizio del rapporto di cura. Il consenso deve essere "esplicito". Riguarda l'autorizzazione che il paziente dà al medico ad utilizzare i suoi dati personali per finalità di diagnosi e cura. Si consiglia la raccolta del consenso in forma scritta, non a voce o "flaggando" la rispettiva voce nel software. Non serve rinnovarlo (va integrato se si utilizzano i dati per altre finalità con una ulteriore firma); può essere revocato in ogni momento. I trattamenti effettuati dal Titolare sulla base del consenso rimarranno comunque legittimi.

Nei pazienti minorenni il consenso deve essere espresso dai genitori o da chi ne esercita la potestà genitoriale o dal tutore.

Se i genitori sono separati o divorziati devono tutelare la salute dei figli, hanno il diritto ad essere informati sullo stato di salute dei figli e il medico deve portare a loro conoscenza dei dati di cui dispone o congiuntamente o disgiuntamente. E' responsabilità dei genitori relazionarsi tra di loro.

Per i medici che si avvalgono di personale di studio devono redigere una lettera formale di incarico al trattamento dei dati a cui si devono attenere.

Medesimo formale incarico va anche affidato al consulente fiscale/commercialista.

Il medico che dispone la raccolta e archiviazione dei dati deve adottare su computer le misure e cautele atte ad evitare o minimizzare i rischi da furto, sottrazione, smarrimento, manomissione o alterazione dei dati.

Se ciò avvenisse, il medico deve poter dimostrare di aver messo in atto tutte le cautele possibili.

Quali accorgimenti tecnici devono essere posti in atto: Computer deve essere protetto da password (la meno intuitiva possibile) che deve essere modificata ogni tre mesi, deve essere installato un antivirus anti malware e se connesso ad internet anche da un firewall che devono ovviamente esser costantemente aggiornati.

E' fondamentale il salvataggio periodico dei dati e la procedura di eventuale ripristino. Il proprio consulente informatico saprà aggiornarvi per rendere il computer sempre protetto.

Accesso ai dati da parte del personale di segreteria: deve accedere con proprio nome utente e una propria password solo ai dati necessari a svolgere il proprio ruolo (indirizzo , telefono ecc..) non ai dati sanitari.

Accesso ai dati da parte di un sostituto: Il sostituto può accedere ai dati utilizzando un proprio nome utente e una propria password in modo che rimanga traccia informatica di chi, come e quando ha fatto l'accesso al sistema.

Accesso ai dati per i medici associati/gruppo/rete : nell'informativa deve essere esplicitata la presenza di queste figure

Diritti del paziente: ha diritto a sapere quali dati che lo riguardano sono in possesso del medico, ha diritto di verificare che tali dati siano esatti e corretti, ha diritto a chiedere la cancellazione (**diritto all'oblio**) in tutto o parte dei dati e ha diritto ad ottenere una copia di tutti i dati che lo riguardano.

Richiesta del paziente di cancellare tutti i suoi dati (Diritto all'Oblio): nell'informativa deve essere esplicitato che se il paziente rifiuta di fornire i dati al medico o se ne chiede la cancellazione è come se revocasse il consenso per cui il medico ne prende atto e può considerare terminato il rapporto fiduciario.

Il medico non può opporsi alla richiesta del paziente di ottenere una stampa o copia dei propri dati sanitari.

Portabilità dei dati: Il nuovo regolamento introduce il diritto alla "portabilità" dei dati personali per trasferirli da un titolare del trattamento ad un altro.

Consegna di documenti sanitari (certificati e/o ricette): possono essere consegnati anche dal personale di segreteria in busta chiusa individuando l'interessato al ritiro, se si tratta di un delegato si dovrà acquisire la delega. I documenti sanitari, anche se chiusi in busta, non possono essere lasciati ad esempio in un scaffale o scrivania in sala di attesa.

Richiesta di dati e informazioni sanitarie da parte di altri soggetti: Vale la regola per cui senza consenso del diretto interessato, il medico <u>non deve comunicare nulla a nessuno.</u>

Dati forniti a terzi senza consenso: sono previsti da norme di legge (nazionali o regionali). Esempio se obbligo di referto, trasmissione scheda malattie infettive, ricettazione come controllo della spesa sanitaria, minore oggetto a maltrattamenti.

Conservazione dei dati: I dati vanno conservati per il tempo necessario al perseguimento della finalità per cui sono stati raccolti. Pertanto si conservano finché dura il rapporto di cura, e poi a norma del Codice Civile conservati per almeno 10 anni.

Il pediatra che cessa l'attività: la cessazione dell'attività corrisponde alla cessazione del rapporto di cura, da quel momento decorrono 10 anni. Infatti potrebbero insorgere contestazioni, vertenze tra medico e paziente, la conservazione permette al medico di conservare le prove della propria correttezza.

Nei certificati: di norma non deve essere riportata la diagnosi; nei minori si deve fare la notifica di malattia infettiva alla ULSS e non alla scuola che non può pretendere certificati di malattia con la diagnosi ma solo di riammissione.

Violazione dei dati (data breach): il Titolare dovrà comunicare eventuali violazioni dei dati personali all'autorità nazionale di protezione dei dati. Se la violazione rappresenta una minaccia per i diritti delle persone si dovrà informare anche i diretti interessati. Siamo esentati da informare gli interessati se riteniamo che la violazione non comporti un rischio elevato per i loro diritti (furto identità, danno immagine ecc..) oppure se possiamo dimostrare di aver adottato misure di sicurezza a tutela dei dati violati.