Nuovo Regolamento europeo sulla Privacy

Il 25 maggio 2018 diventa applicabile il **Regolamento europeo sul trattamento dei dati personali** (679/2016). Tale Regolamento contiene nuove regole privacy, nonché i nuovi standard di protezione dei dati.

Tale data non è e non sarà oggetto di proroga. Si tratta di un Regolamento Europeo e, come tale, sarà applicabile in tutti gli Stati Membri dell'Unione.

Il Regolamento si applica a tutti i soggetti pubblici o privati che attuano un trattamento dei dati, per cui si applica anche alle strutture sanitarie e agli studi professionali e in particolare incide sul trattamento di tutte le informazioni e i dati che lo studio medico, odontoiatrico e professionale ottiene dai pazienti, sul modo in cui lo studio interagisce con questi dati e sul modo in cui li conserva.

Le principali novità sono le seguenti.

Liceità del trattamento dei dati e condizioni per la manifestazione del consenso

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Il consenso deve essere esplicito per i dati "sensibili", fra i quali vi sono i dati relativi allo stato di salute.

Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

L'informativa

Il titolare deve sempre specificare la base giuridica del trattamento, cioè la motivazione alla base della raccolta dei dati.

Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

La nomina del Responsabile della Protezione dei Dati (RPD)

Una delle novità più importanti del Regolamento Europeo è la nomina di un Responsabile della Protezione dei Dati (RPD in italiano, DPO in inglese).

Questo soggetto deve essere in possesso di adeguate capacità professionali, in particolare, della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali e ha il compito di aiutare a mantenersi conformi alle nuove regole sulla protezione della privacy.

Il DPO funge anche da intermediario con le autorità di controllo, in particolare l'autorità giudiziaria ed il Garante della Privacy.

La nomina del RPD è obbligatoria per tutti gli Enti Pubblici, nonché per le attività il cui esercizio comporta la manipolazione di dati in "larga scala" per speciali categorie di dati, tra i quali i dati sanitari. Per gli studi medici tale nomina non è obbligatoria, anche se tutti i commentatori la consigliano vivamente per supportare il titolare dello studio nell'adempimento degli obblighi sulla privacy.

La funzione di RPD può essere svolta da un fornitore esterno di servizi purché sia esercitata sulla base di un contratto stipulato tra il titolare dello studio ed una persona fisica oppure giuridica, quindi una società. Per fare un esempio: lo studio medico delega la responsabilità al fornitore del proprio software gestionale (attraverso un accordo sul trattamento dei dati), che nominerà un RPD per tutti i dati contenuti nei propri server e gestiti attraverso il software. Ma occorre fare attenzione, poiché questo sarà possibile solo nel caso in cui il gestionale sia un software in cloud, dato che la tecnologia cloud permette di controllare da remoto tutti i dati dello studio. Per tutti gli altri eventuali dati che lo studio conserva fisicamente sui propri dispositivi (o in cartaceo), invece, il titolare dello studio deve conformarsi alle norme sancite dal Regolamento sotto la propria responsabilità, eventualmente nominando il RPD.

Le violazioni

In caso di violazioni, il titolare risponde personalmente delle violazioni commesse poiché spetta al titolare rispettare la normativa e controllare chi effettivamente ha accesso ai dati dei pazienti, chi modifica o inserisce dati fiscali e di salute su un documento digitale o cartaceo.

Il RPD risponde della mancata realizzazione dei suoi compiti, quindi di consulenze errate o non efficaci rispetto al contratto stipulato e soprattutto risponde delle proprie violazioni riguardo alla normativa europea sul trattamento dei dati personali.

Strumenti operativi

L'Autorità Garante dovrebbe mettere a disposizione alcuni strumenti operativi di riferimento, come ad esempio il modello standard per l'informativa per gli studi medici e il modello standard per la raccolta del consenso esplicito, aggiornando quanto pubblicato nel 2006.

Si resta in attesa di tali determinazioni.