

Torino, 20 maggio 2018

NUOVE REGOLE SULLA PRIVACY PER I MEDICI CHIRURGHI E GLI ODONTOIATRI

Il 25 maggio 2018 scatterà il termine per tutti per l'adeguamento alle nuove norme sulla privacy introdotte dal Regolamento UE n. 2016/679, sulla cui modalità di attuazione regna tra gli odontoiatri molta confusione.

Pochi sanno che cosa è necessario fare per mettersi in regola. Cercheremo quindi di fornire qualche semplice indicazione per consentire di non farsi trovare impreparati.

Il Regolamento è un documento molto complesso, ma lo stesso riserva ai singoli professionisti alcuni adempimenti che semplificati al massimo possono essere sintetizzati in 5 o 6 adempimenti: documentare l'analisi dei rischi, aggiornare le informative e i consensi, predisporre il registro dei trattamenti, mettere in sicurezza i propri elaboratori, informare e formare i propri collaboratori.

Più complessa la situazione delle associazioni professionali e delle società tra professionisti per i quali sembra necessaria la nomina di un responsabile della protezione dei dati o la stesura del documento di valutazione d'impatto.

Cosa devono fare il medico e l'odontoiatra?

Innanzitutto prendere coscienza che qualunque sia la forma di esercizio della sua professione (consulente, collaboratore, titolare di studio, etc.) è un soggetto che tratta dei dati, dati di categoria molto delicata, e di conseguenza è tenuto ad osservare le nuove regole sulla privacy.

IL REGISTRO dei TRATTAMENTI

E' il primo documento che deve essere compilato, il quale contiene la mappatura dei trattamenti eseguiti dal professionista. Coloro che hanno compilato il Documento Programmatico sulla sicurezza obbligatorio fino al 2012 hanno un buono schema tra le proprie carte. Il Registro può essere elaborato su uno schema base, su un modello valido per tutti gli appartenenti alla categoria.

Esso dovrà contenere la specificazione di come vengono raccolti, trattati, conservati i dati dei clienti, i soggetti che sono legittimati al trattamento e di tutto ciò che interessa i dati.

SICUREZZA

E' questo un aspetto molto spinoso. Il professionista deve garantire che tutti i dati conservati nello studio siano messi in sicurezza. Come? Con server crittografati, sistemare i backup degli elaboratori,

inserire password che dovranno essere cambiate con periodicità, assicurarsi della validità degli antivirus, conservare cartelle cartacee in armadi chiusi a chiave, etc.

Per assolvere a questo onere è dunque necessario fare un'attenta analisi dei rischi e degli strumenti elettronici e non. Ci sono ancora alcuni aspetti da chiarire in merito a chi deve fare alcuni nuovi adempimenti su cui si attendono chiarimenti dal Garante.

DIPENDENTI e COLLABORATORI

I dipendenti e i collaboratori dovranno essere designati in modo formale "autorizzati al trattamento" mediante uno specifico documento. L'adempimento è simile alla vecchia designazione di "incaricati del trattamento".

INFORMATIVE

Questo è un adempimento conosciuto. I professionisti devono dare informativa privacy ai propri clienti. Dovranno in sostanza dire come verranno trattati i dati e quale sarà la loro sorte, chi potrà trattarli, etc.

E' un adempimento che si colloca nella fase iniziale del rapporto in cui il medico e l'odontoiatra sono tenuti a svariati adempimenti prima di iniziare a curare: informare il paziente del tipo di terapia, stendere un preventivo e/o contratto di incarico professionale, raccogliere il consenso informato alle cure in forma scritta (L. 219/2017) e raccogliere il consenso al trattamento dei dati.

Si ricorda che il nuovo Regolamento rinnova e amplia i contenuti dell'informativa.

CONSENSO

E' questo un argomento che lo Stato Italiano dovrà regolare entro il 21.5.2018 in quanto il Regolamento U.E. lascia ai singoli Stati libertà di disciplina.

Il discorso non è di poco conto perché per i dati sanitari che sono quelli trattati dai medici e dagli odontoiatri, il Regolamento prevede la possibilità di loro trattamento senza consenso. Occorre quindi attendere cosa dirà il legislatore italiano sull'argomento.

RAPPORTI CON I COMMITTENTI

Non è esplicitamente previsto se professioni debbano farsi nominare responsabili del trattamento dai propri committenti che trasferiscono dati di persone fisiche. L'aspetto è particolarmente rilevante a fronte della necessità di sottoscrivere un contratto e della responsabilità civile solidale (tra titolare e responsabile esterno del trattamento). In materia i Garanti europei (riuniti nell'organismo chiamato WP29) hanno affermato che la questione dipende dal grado di autonomia nell'esecuzione dell'incarico.

Nella prassi, probabilmente, la gestione dei dati per conto di un cliente sposta verso la qualifica del professionista come responsabile esterno.

CODICI DI CONDOTTA

Il regolamento UE 2016/679 sollecita gli organismi rappresentativi di categorie, come quelle professionali, a scrivere un codice di condotta "privacy", da far approvare dal Garante.

Serve per avere certezze sugli adempimenti e per diminuire la responsabilità.

Le professioni hanno tutto l'interesse a definire al più presto questo codici.

TABELLA GLI ADEMPIMENTI DEI PROFESSIONISTI

Adempimenti	Indicazioni operative	Questioni aperte
Nomina DPO	Non obbligatoria per singolo professionista (non opera su larga scala)	Chiarire se gli studi associati obbligati alla nomina del DPO
Registro trattamenti	Non obbligatoria per gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio	Chiarire se obbligatorio per professionisti, studi associati e società tra professionisti
Base giuridica del trattamento di dati comuni	Di regola non necessario il consenso, in quanto vale la base giuridica contrattuale o dell'obbligo di legge	Da chiarire se trattamenti ulteriori possano rientrare nel legittimo interesse
Base giuridica del trattamento di particolari categorie di dati	Di regola necessario il consenso; il regolamento UE non richiede il consenso per i trattamenti di rapporti di lavoro e per i trattamenti sanitari	Chiarire se le autorizzazioni generali del Garante sul trattamento di dati sensibili per i professionisti saranno ancora valide Definire norme di coordinamento e armonizzazione
Informativa	Osservanza obbligatoria da parte di tutti i professionisti	In attesa di indicazione di "icone" ufficiali da abbinare all'informativa discorsiva
Diritti interessato	Osservanza obbligatoria da parte di tutti i professionisti	Chiarire se la portabilità dei dati significhi trasferimento integrale del fascicolo informatico del cliente
Analisi dei rischi	Osservanza obbligatoria da parte di tutti i professionisti	Non ci sono modelli base di riferimento

Adeguamento elaboratori ed altri strumenti con cui si trattano dati	Osservanza obbligatoria da parte di tutti i professionisti	Non ci sono regole tecniche standard
Nomina responsabili esterni	Osservanza obbligatoria da parte di tutti i professionisti	In attesa di clausole tipo da parte del Garante
Nomina autorizzati al trattamento	Osservanza obbligatoria da parte di tutti i professionisti	Obbligo coincidente con la designazione degli incaricati di trattamento
Valutazione di impatto privacy	Non richiesta per trattamenti di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o odontoiatra	Chiarire se obbligatorio per studi associati e società tra professionisti
Data breach	Osservanza obbligatoria da parte di tutti i professionisti	Chiarire casi di esonero
Codici di condotta	Da elaborare dalle associazioni rappresentative	In attesa di definizione di codici di condotta di categoria
Sanzioni	Applicabili a tutti i professionisti	

SANZIONI

Si evidenzia da ultimo che la mancata osservanza delle nuove disposizioni sulla privacy comporta sanzioni amministrative di natura economica molto pesanti.