# Le novita' normative sulla privacy sanitaria

**Data** 28 giugno 2019
**Categoria** medicina_legale

Il Garante Privacy ha fornito le indicazioni sull'applicazione del regolamento Ue sulla protezione dei dati (Gdpr) in ambito sanitario con il provvedimento n. 55 del 7 marzo 2019, chiarendo alcuni aspetti del D.Lvo 101/2018.
Alcuni chiarimenti davvero utili, ma restano delle zone d' ombra...

Va considerato in primo luogo che il singolo medico non deve nominare il Dpo (responsabile della protezione dei dati).

Il professionista sanitario, in virtu' del segreto professionale, non deve piu' richiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dal fatto che operi in uno studio medico o in una struttura sanitaria pubblica o privata.
La norma, tuttavia, vale solo per i trattamenti necessari alle cure. Per altri trattamenti "collaterali" dei dati riguardanti sia i medici che le strutture sanitarie in genere (servizi amministrativi, iniziative aventi finalita' commerciali o elettorali, fidelizzazione della clientela con app mediche o raccolta punti) serve uno specifico consenso dell' intreressato.

Riguardo alle aziende sanitarie il Garante suggerisce di fornire le informazioni in maniera progressiva fornendo alla generalita' dei pazienti le informazioni relative ai trattamenti rientranti nelle ordinarie prestazioni sanitarie, riservando le informative relative a particolari attivita' di trattamento solo ai pazienti effettivamente interessati da tali servizi.
Le aziende sanitarie devono nominare il Dpo ( responsabile della protezione dei dati, indicato anche con la sigla Rpd).
La norma vale anche per gli ospedali privati, le case di cura e per le RSA (residenza sanitaria assistenziale).
Il singolo professionista sanitario operante in regime di libera professione a titolo individuale, non dovrà nominare un Dpo. L' obbligo scatta per farmacie, parafarmacie e aziende ortopediche e sanitarie solo nel caso di effettuazione di trattamenti su larga scala.

Gli operatori sanitari devono compilare il "Registro delle attivita' di trattamento" che dovra' essere compilato sia dai singoli professionisti sanitari, i medici di medicina generale e i medici pediatri, gli ospedali privati, le case di cura, le Rsa, le aziende del servizio sanitario, le farmacie, le parafarmacie e le aziende ortopediche. Dovra' riportare le attivita' effettuate sotto loro responsabilita'.
Il registro non va trasmesso al garante, ma conservato per eventuali controlli delle autorita'.

Puntualizzazioni e commenti:
Il chiarimento del Garante ha lasciato alcune zone d' omra riguardanti soprattutto i medici di base operanti in associazioni o gruppi. Non è stato infatti ancora pienamente definito lo stato giuridico, delle varie forme di associazionismo ne' c'e' una norma precisa che indichi di chi sia ad oggi la responsabilità della nomina del DPO, né quando può definirsi “larga scala” la quantità dei dati trattati.

Infatti per i diversi studi associati in base alle vigenti Convenzioni, secondo il regolamento, potrebbero configurarsi casi diversi: un caso frequente riguarda gruppi di medici che condividono unicamente i locali, restando ogni medico responsabile del trattamento sanitario e dei dati dei propri pazienti (mentre i colleghi intervengano sotto la veste di sostituti), la situazione non differisce dal medico singolo.
Se invece i medici condividono i dati in unico software e/o server e li scambiano in un sistema esteso e comune di presa in carico e di condivisione dei dati, andrebbero considerati (almeno fino ad ulteriore chiarimento del garante) come trattamento in "larga scala" che implicherebbe la nomina del Dpo. Come ho gia' detto, mancano a tale proposito chiare e precise disposizioni, auspicabili considerando l' entita' e la gravita' delle sanzioni previste.

Se il sanitario (vale soprattutto per i laboratori, ma puo' interessare anche altri) spedisce i referti all’assistito via e-mail devono essere garantiti certi requisiti: spedire il referto in forma di allegato e non come testo compreso nella body part del messaggio e proteggere il file con password o in una chiave crittografica stabilita dalle due parti tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B al Codice).
Ma occorrerà anche che gli indirizzi e-mail siano validati con apposita procedura di verifica on-line, così da evitare di spedire documenti elettronici, pur “cifrati”, a soggetti diversi dall’assistito.

Viene richiesto spesso al medico di rilasciare informazioni su pazienti deceduti: ricordiamo che i dati di soggetti deceduti (articolo 2 terdecies D.Lvo 101/2018) possono essere attinti da chi ha un interesse proprio o a tutela dell'interessato, o per ragioni familiari da proteggere, ma non se l'interessato lo ha vietato con dichiarazione scritta all'ospedale. In quest'ultimo caso, pero', il divieto non può pregiudicare i diritti degli eredi o di titolari di interessi da difendere in giudizio

DanieleZamperini