Il GDPR per la privacy nella sanità privata

Mancano ormai solo 8 mesi all'attuazione del nuovo Regolamento UE 679/2016 sulla Protezione dei Dati Personali (o *General Data Protection Rule*, GDPR), pubblicato nel maggio 2016, che diverrà pienamente attuativo il 25 maggio 2018. Esso apporta importanti novità alla Legge sulla Privacy italiana attualmente in vigore, il D. Lgs 196/2003 e s.m.i., ed impone un diverso modo per affrontare la privacy nelle organizzazioni che trattano dati sanitari, i quali costituiscono una particolare categoria di "dati sensibili" (ora definiti "dati particolari" dal GDPR).

In questo articolo ci occuperemo delle regole per la privacy dei dati sanitari secondo il GDPR, ma non di ciò che attiene alla Sanità Pubblica, quali Ospedali, ASL, ambulatori pubblici, ecc., i quali dovranno sottostare alle medesime regole, ma con adempimenti leggermente diversi (ad es. la figura del DPO o *Data Protection Officer* è obbligatoria sempre) e con l'identificazione del titolare del trattamento che investe un'entità della Pubblica Amministrazione. Da un certo punto di vista lo Stato ha mezzi adeguati per affrontare, speriamo nel modo corretto, l'adeguamento al GDPR.

Invece, per quanto riguarda la Sanità Privata, le cose sono un po' diverse ed a volte l'organizzazione interna non contempla competenze e tecnologie adeguate per far fronte al nuovo Regolamento 679/2016. Parliamo di organizzazioni di piccole e medie dimensioni, che vanno dalle Farmacie ai Poliambulatori di analisi diagnostiche, alle Cliniche e Case di Cura Private.

Alcuni adempimenti nelle organizzazioni private che si occupano di servizi sanitari sono da interpretare, in quanto la norma europea non fornisce indicazioni così precise su alcuni aspetti, ma pone l'accento sulla "responsabilizzazione" del titolare del trattamento, ovvero sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, cioè misure tecniche ed organizzative adeguate.

Ci troviamo così di fronte ad un problema di competenze: il titolare del trattamento di queste organizzazioni della Sanità Privata è la società stessa che gestisce la struttura (a volte il singolo professionista), quindi tutte le responsabilità ricadono, di fatto, sul legale rappresentante della stessa, il quale normalmente si occupa di tutt'altro (medico, farmacista o manager amministrativo) e non sa quali misure adottare per tutelarsi, non solo dalle possibili sanzioni (fino al 4% del fatturato annuo), ma anche da eventuali richieste di risarcimento danni di pazienti che non sentissero adeguatamente tutelata la propria privacy.

Gli elementi da considerare nella gestione della privacy in una organizzazione sanitaria privata sono diversi: la gestione dei documenti su supporto cartaceo o analogo (es. lastre di esami diagnostici), la gestione dei documenti su supporto digitale, la gestione delle informazioni elaborate dai sistemi informatici, la gestione delle informazioni trasmesse verbalmente…

Coloro che hanno gestito la privacy in passato con l'aiuto di un avvocato – che gli ha preparato lettere di nomina incaricati, informative e consensi – e di una società di consulenza informatica – che gli ha gestito la sicurezza dei dati (antivirus, backup, ecc.) – dovranno modificare il proprio approccio in quanto la nuova privacy del GDPR richiede un approccio più sistemico ed orientato alla valutazione dei rischi.

I principi introdotti dal GDPR – in particolare il principio di liceità del trattamento, di integrità e di riservatezza, di limitazione delle finalità… – devono essere recepiti interpretandoli nel modo corretto, declinandoli nella propria realtà; non esistono più regole ben definite (password di almeno 8 caratteri, antivirus aggiornati con una certa frequenza, ecc.).

I passi fondamentali che un'organizzazione sanitaria privata dovrebbe affrontare per adeguarsi al GDPR sono i seguenti:

- Analisi dei processi dell'organizzazione;
- Mappatura dei trattamenti di dati personali;
- Identificazione di ruoli e responsabilità per il trattamento;
- Predisposizione del Registro dei trattamenti di dati personali;
- Valutazione dei rischi sui trattamenti di dati;
- Valutazione di impatto per quei trattamenti che lo richiedono;
- Definizione delle misure organizzative per la protezione dei dati personali;
- Definizione delle misure tecniche per la protezione dei dati personali;
- Predisposizione delle procedure per il trattamento dei dati e loro documentazione.

In questo percorso si incontrano alcuni elementi particolarmente significativi, la cui gestione richiede molta attenzione ed una corretta interpretazione del Regolamento 679/2016:

- La formulazione dell'**informativa** e dei **consensi** al trattamento da parte degli interessati;
- La progettazione, implementazione e gestione della **sicurezza delle informazioni** (non solo informatica);
- Gestione degli **applicativi informatici** e dei rapporti con i relativi fornitori;

- Rapporti con i **responsabili del trattamento esterni**;
- Eventuale **nomina del DPO** o RPD (Responsabile del Trattamento dei Dati);
- Modalità di effettuazione della **valutazione dei rischi** e necessità del c.d. *Data Impact Assessment* (DIA).

Vediamo di chiarire un paio di punti relativamente alle organizzazioni sanitarie private.

La nomina del DPO (RPD) è obbligatoria:

1. se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
2. se le attività principali del titolare o del responsabile consistono in **trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala**;
3. se le attività principali del titolare o del responsabile consistono nel **trattamento su larga scala di categorie particolari di dati** o di dati personali relativi a condanne penali e reati.

Se è evidente che non siamo nel caso (a), probabilmente nemmeno nel caso (b), occorre riflettere bene sul caso (c).

I dati sanitari ricadono senz'altro nelle particolari categorie di dati definite dal GDPR e resta solo da capire cosa significa "su larga scala". Le interpretazioni ufficiali (Regolamento e Linea Guida sui RPD del GdL Articolo 29) ci indicano che i pazienti trattati da un singolo medico di famiglia non rientrano nel concetto di "larga scala". Analogamente si potrebbe pensare per una Farmacia o un piccolo ambulatorio privato, ma salendo di dimensione nelle organizzazioni è evidente che questa condizione trova applicazione.

Altra questione è quella relativa alla necessità di istituire un **Registro dei Trattamenti**: qui l'obbligo si ha per organizzazioni con più di 250 addetti oppure in presenza di

rischio per diritti e libertà degli interessati per trattamenti non occasionali di dati sensibili o giudiziari. In questo caso le nostre organizzazioni della sanità privata ricadono quasi tutte nell'obbligo di trattamento, fermo restando che è comunque opportuno, per il principio di responsabilizzazione (*accountability*) del titolare del trattamento, creare e gestire tale Registro.

Esiste, infine, la possibilità, per i titolari del trattamento che vorranno garantirsi maggiormente dai rischi inerenti la privacy, di ottenere la certificazione del proprio processo di gestione di dati sanitari (per ora solo lo Schema di Certificazione ISDP©10003:2015 di INVEO, accreditato da ACCREDIA).