privacy verso nuove regole: *cosa cambia in sanità?*

di Umberto Marchi

Cambio di rotta, o, se si preferisce, giro di vite sulle regola in materia di privacy. Il prossimo 25 maggio 2018 scatterà l'ora "x" del nuovo Regolamento europeo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Ue 2016/679). Si tratta di una normativa più complessa della precedente, e molto cambierà anche in sanità.

E' in arrivo una rivoluzione -o meglio, un'evoluzione- nel complicato territorio della normativa sulla privacy: infatti dal 25 maggio prossimo le nuove disposizioni sul trattamento dei dati personali recepite dall'Europa (Regolamento UE 2016/679) manderanno in soffitta il vigente (ancora per poco) Codice della privacy, che a dire il vero è un po' vecchiotto, visto che risale a 15 anni fa, cioè al 2003.

Regole più complesse

Il nuovo Regolamento è più complesso rispetto al sistema normativo previgente, e si adatta ai numerosi mutamenti che in questi anni si sono verificati. Molti sono gli ambiti di intervento: più nello specifico, disciplina la contitolarità del trattamento e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente; fissa più dettagliatamente rispetto alle norme ora in vigore le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento; consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile"; prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti; l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti; la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale. Un'importanza particolare è data al principio della responsabilizzazione (accountability) di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

La sanità coinvolta in pieno

E' evidente come la sanità non possa essere esente dal conoscere ed applicare in maniera corretta le nuove disposizioni. Anzi, è proprio in sanità che si registra, forse, il più alto tasso di dati

sensibili. Infatti il cittadino che si rivolge alle strutture sanitarie ha diritto alla più totale riservatezza su diagnosi, cure, prestazioni mediche e altro. Detto questo, cosa cambia? E come procedere? Partiamo dalle due categorie sanitarie a cui il Regolamento è indirizzato, vale a dire gli esercenti le professioni sanitarie e gli organismi sanitari. La prima cosa, ovviamente, è conoscere il Regolamento.

Dall'analisi del rischio al Registro Trattamenti

Una volta presa confidenza con la nuova disciplina, occorre una mappatura precisa dei dati, del perché si trattano e come si trattano. Il Regolamento, infatti, richiede una fase di analisi del rischio dei dati trattati, per poi redigere il Registro dei Trattamenti secondo il nuovo articolo 30. Un principio parzialmente nuovo introdotto dal Regolamento è quello secondo il quale l'interessato deve avere il controllo dei propri dati. Ergo, l'informativa deve essere chiara, completa ed esaustiva, e consentire (anche mediante l'utilizzo, ad esempio, di icone) all'interessato di decidere se e come permettere il trattamento dati.

Valutare la necessità di riorganizzazioni interne

Oltre al diritto di sapere e poter decidere, non deve sfuggire quello di controllare (ad esempio procedere alla limitazione del trattamento, alla revoca del consenso). Sono tutelati anche il diritto all'oblio e quello alla portabilità dei dati. A questo punto, l'ospedale o la struttura sanitaria devono verificare l'adeguatezza delle procedure interne nell'ottica di garantire il rispetto di tutti questi diritti, valutando la necessità di riorganizzazioni e ristrutturazioni interne.

Il consenso esplicito

Cambia anche l'approccio al consenso, che in un certo senso risulta semplificato: non più scritto o verbale, ma libero (non condizionato), specifico (uno per ogni finalità), inequivocabile (certo) ed espresso. In caso di dati sensibili dev'essere anche esplicito, e resta in capo al titolare dei dati la prova di avere correttamente acquisito il consenso.

Parola d'ordine: responsabilizzazione

Fondamentali attività sono quelle connesse al rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. A questo proposito occorre rivedere il processo di gestione della Asl, ospedale o struttura sanitaria. Anche perché il Regolamento introduce l'obbligo in capo al Titolare di implementare un sistema organizzativo coerente con la privacy by design e by default. Insomma, il rispetto dei principi privacy è insito nella organizzazione del servizio o del prodotto ad origine ed in via predefinita. Ove poi l'erogazione del servizio sanitario possa impattare fortemente sulla tutela dei dati va effettuata una valutazione di impatto.

Il DPO, una nuova figura con molte competenze

Ancora: tra gli adempimenti di più ampio impatto sul mercato vi è certamente la designazione del responsabile della protezione dei dati personali ovvero del Data Protection Officer (DPO), figura che diverrà obbligatoria per tutta la pubblica amministrazione e in alcuni casi anche in ambito privato. Si tratta di una figura nuova, chiamata a svolgere in parte attività di consulenza e formazione ed in parte attività di controllo. Deve unire competenze di varia natura: dalla conoscenza del Regolamento nuovo a quelle più specificatamente tecniche e tecnologiche. Cambiano anche le regole sul trasferimento dati, con disposizioni specifiche in caso di app, cloud e manutenzione da remoto. Già presente nel provvedimento del Garante sul Dossier sanitario è il "data breach", che però viene esteso dalle nuove regole a tutti i trattamenti. Necessario anche comunicare eventuali violazioni di dati e/o sistemi. Le sanzioni per chi non lo fa? Fino a 20milioni di euro e/o il 4% del fatturato aziendale. C'è poco da scherzare.