I rischi specifici **connessi al trattamento dei dati sanitari**

Il complesso quadro normativo e la crescente necessità di sicurezza dei dati.

Maddalena Valli
avvocato

KEYWORDS
dati sensibili, dati sanitari, privacy
sensitive data, health data, privacy

I dati sanitari sono costituiti, nella nuova definizione che possiamo trarre dal Regolamento Europeo n. 679/2016 ("GDPR"), entrato in vigore lo scorso 25 maggio 2018, dall'insieme delle informazioni personali in grado di rivelare lo stato di salute, la vita sessuale, le condizioni fisiche e mentali di un soggetto, ivi inclusi i dati genetici, i referti medici, le analisi cliniche e il materiale fotografico e video raccolto a fini diagnostici nonché per la preparazione e l'esecuzione di interventi chirurgici.

Devono quindi essere considerati dati sanitari tutti i dati prodotti dai servizi di assistenza sanitaria che rivelano informazioni relative allo stato di salute di una persona e, inoltre, tutti quei dati generati da dispositivi o da applicazioni utilizzati per la conoscenza del proprio stato di salute e ciò indipendentemente dalla qualificazione di "dispositivo medico" della tecnologia che li ha generati.

La tutela del paziente dovrà tuttavia rapportarsi sempre più spesso e in modo organico e costruttivo alla tutela della collettività. Il GDPR, in tale ottica, ha sancito che i dati sanitari possono essere utilizzati per finalità connesse alla salute (finalità di cura), per la supervisione del Sistema Sanitario Nazionale (finalità di governo) e per la ricerca nel pubblico interesse. La normativa in materia di gestione dei dati sanitari è complessa ed è basata, oltre che su leggi nazionali (Codice Privacy) e su provvedimenti di carattere generale dell'Autorità Garante, anche su leggi promulgate dalle Regioni nell'ambito dell'autonomia garantita loro a partire dal 1970 e confermate nella riforma costituzionale del 2001. Da ultimo, a ciascuno Stato membro della Ue, è stata concessa dal legislatore europeo la possibilità di introdurre condizioni particolari o ulteriori limiti in materia di dati "particolari", definizione questa che ha sostituito quella più nota di "sensibili".

L'art. 13 della legge di delegazione europea 2016-2017 ha demandato al Governo italiano il difficile compito di adottare i provvedimenti necessari ad adeguare il quadro normativo nazionale al GDPR: tali decreti attuativi dovevano essere emessi entro il 21 agosto 2018. Si auspica possano fornire i necessari e opportuni chiarimenti anche nell'ambito del complesso trattamento dei dati sanitari, all'interno del progetto organico di riorganizzazione della sanità europea già in atto, che dovrà portare alla gestione unificata in ambito UE (National Contact Point for eHealth – NCPeH) ovvero all'auspicata interoperabilità e allo scambio transfrontaliero del Patient Summary (profilo sanitario sintetico) oltre che dell'ePrescription (ricette mediche elettroniche).

In tale contesto, l'aumento della quantità e del grado di sensibilità dei dati personali e sanitari, unitamente allo sviluppo tecnologico, hanno incrementato il rischio che un trattamento incauto e non professionale di dati sanitari possa determinare danni per gli interessati e respon-

The complex regulatory framework and the growing need for data security.

sabilità per i soggetti della filiera del trattamento.
Come chiarito da Antonello Soro, presidente del Garante per la protezione dei dati personali (intervista di Ruggiero Corcella, Corriere della Sera, 6 marzo 2017): I dati sanitari, se illecitamente trattati o addirittura "rubati", sono suscettibili di esporre l'interessato a forme di discriminazione pericolose, rese possibili dalla conoscenza degli aspetti più intimi della persona, come quelli "idonei a rivelare lo stato di salute dell'interessato". La sottrazione o peggio l'alterazione di un dato sanitario, inoltre, rende vulnerabili banche dati essenziali per il governo del nostro Paese, si pensi ai sistemi informativi sanitari delle Asl, delle Regioni o del Ministero della Salute, che sono indispensabili per la gestione della sanità pubblica. Ma soprattutto, la vulnerabilità del dato sanitario e, quindi, la suscettibilità di alterazione o modificazione di queste informazioni, rischia di determinare errori diagnostici o terapeutici, con conseguenze anche letali per l'interessato e gravi responsabilità per gli stessi operatori sanitari".
Nella progettazione e/o uso di software in ambito sanitario non si può quindi prescindere da un'attenta analisi di ogni aspetto logico, tecnico, organizzativo e normativo al fine di limitare il più possibile i summenzionati rischi di trattamento illecito dei dati.

Progettazione e utilizzo di software in ambito sanitario: i principali aspetti da considerare anche alla luce del GDPR

È fondamentale procedere innanzitutto all'esatta individuazione del Titolare del Trattamento dei dati e della filiera a questi collegata. Fermo restando che il medico o la struttura sanitaria (pubblica o privata che sia) non sono mai "proprietari" dei dati dei pazienti, al fine di non incorrere in un illecito trattamento dei dati sanitari è indispensabile analizzare e specificare, in modo chiaro e trasparente nei confronti dei pazienti, i ruoli di tutti i soggetti coinvolti nel trattamento.
Le strutture sanitarie, allorché siano esclusive titolari del dato del paziente, dovranno porre ogni opportuna cautela affinché il personale medico e paramedico non utilizzi software personali (quindi non autorizzati dalla struttura sanitaria) per trattare i dati dei pazienti. Anche in quest'ottica, le strutture sanitarie dovranno quindi dotarsi di sistemi gestionali che, sfruttando l'innovazione tecnologica, garantiscano il rispetto della complessa normativa italiana ed europea.
Ciò influirà non solo sulla possibilità di trattamento di dati da parte di medici, inseriti nelle strutture sanitarie ma non titolari del trattamento, mediante software all'interno di device cd. "privati", ma anche nella redazione di progetti di studio o di sperimentazione clinica.
Viene qui in considerazione anche la necessità per le strutture sanitarie di dotarsi di misure di sicurezza idonee; a tal fine è necessaria un'adeguata verifica e mappatura dei sistemi informatici utilizzati per il trattamento dei dati dei pazienti e sarà quindi necessario valutare con attenzione le banche dati in uso al titolare del trattamento e la contrattualizzazione dei rapporti con i soggetti destinati ad accedere e interagire con le stesse.
La mappatura delle banche dati, unitamente alle relative nomine (incaricati e responsabili del trattamento, amministratori di sistema ecc.), è passaggio imprescindibile per la realizzazione del registro dei trattamenti e la predisposizione della Valutazione d'Impatto (c.d. "DPIA"). Il Re-

gistro del Trattamento, così come la DPIA, sono entrambi istituti di recente introduzione da parte del GDPR.
Le misure di sicurezza non possono essere "minime" (come quelle indicate nel Disciplinare Tecnico Allegato B del "vecchio" Codice Privacy), in forza del principio di accountability introdotto da GDPR, bensì devono essere effettivamente idonee e adeguate (ai sensi dell'art. 32 e segg. del GDPR) per tutelare la sicurezza dei dati. Se è pur vero che i principali obblighi in materia di sicurezza – applicabili a tutti i trattamenti, incluso il mondo sanitario - erano contenuti all'interno del Codice Privacy, che distingueva tra misure idonee e misure minime, non possiamo pensare che le misure minime previste da una normativa del 2003 siano ancora adeguate ed efficaci nel 2018, vista la velocità con cui progredisce la tecnologia.
In tale contesto, anche le Sezioni Unite della Cassazione in una recente pronuncia (Cassazione Civile, SS.UU., sentenza 27/12/2017 n. 30981) hanno precisato che «i dati sensibili idonei a rivelare lo stato di salute possono essere trattati soltanto mediante modalità organizzative quali tecniche di cifratura o criptatura che rendono non identificabile l'interessato. Ne consegue che i soggetti pubblici o le persone giuridiche private, anche quando agiscano rispettivamente in funzione della realizzazione di una finalità di pubblico interesse o in adempimento di un obbligo contrattuale, sono tenuti all'osservanza delle predette cautele nel trattamento dei dati in questione».
Vi sono, inoltre, dei principi cardine che si sono fatti faticosamente strada nella cultura occidentale: sono stati inclusi nella dicitura "Privacy by design", teorizzata in modo organico per la prima volta dalla dott.ssa Cavoukain, membro della Information and Privacy Commissioner of Ontario (Canada) e quindi evolutasi fino alla recente adozione nel GDPR. Implica la progettazione della privacy fin dalla fase di concepimento di un nuovo trattamento di dati personali in modo trasparente e con la centralità dell'interessato. Ciò impone:
(i) una valutazione dell'"impatto privacy" sin dall'origine di nuovi progetti;
(ii) un'adeguata scelta e contrattualizzazione dei fornitori coinvolti;
(iii) l'individuazione e predisposizione di misure logiche, tecniche e organizzative (ovvero procedure e analisi "sul campo", oltre che tecnologie) idonee a minimizzare il rischio di trattamento illecito dei dati, ivi inclusa la definizione di procedure chiare e idonee a definire le modalità di intervento in caso di "data breach" ovvero di violazione dei dati medesimi;
(iv) protezione del ciclo vitale dei dati personali, dalla generazione alla distruzione (ove possibile) degli stessi.
Non va dimenticato, infine, il ruolo fondamentale della formazione: il GDPR riporta alla ribalta l'importanza di un'adeguata formazione in materia di privacy per quanto concerne gli aspetti del trattamento medico e informatico, sia da parte del personale operativo sia da parte dei vertici aziendali e degli Enti Pubblici. Qualsiasi tecnologia è progettata, implementata e soprattutto utilizzata e gestita dall'uomo e non dovrebbe essere analizzata senza valutare la sua interdipendenza da esso. Schneier, uno dei massimi esperti di sicurezza tecnologica, ha aggiornato nei decenni la sua analisi e ci ricorda che: "The single most important factor in security – more than locks, alarms, sensors, or armed guards – is attitude" (Schneier, 2004).

Maddalena Valli, senior manager Legalitax

© RIPRODUZIONE RISERVATA