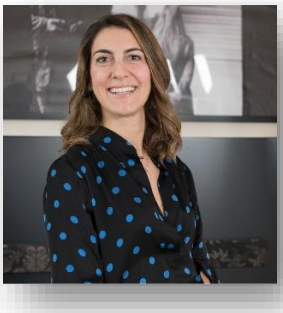
# ***TRATTAMENTO DEI DATI IN AMBITO SANITARIO: I CHIARIMENTI DEL GARANTE***

## *Il Garante Privacy fornisce agli addetti ai lavori i primi chiarimenti sul trattamento dei dati in ambito sanitario*

***Autore***



***Simona Custer***

Con provvedimento n. 55 dello scorso 07.03.2019 l'Autorità Garante per la protezione dei dati è intervenuta in materia sanitaria esprimendosi su tutta una serie di problematiche, oggetto da sempre di numerose segnalazioni e quesiti da parte degli addetti ai lavori.

In particolare, il Garante ha deciso di fornire a tutti coloro che operano nel settore sanitario un supporto nell'attività di adeguamento alle disposizioni contenute nel Regolamento UE n. 2016/679 (di seguito "GDPR") e un'interpretazione univoca della nuova normativa, analizzando i seguenti aspetti: i) trattamento dei dati relativi alla salute in ambito sanitario; ii) informazioni da fornire all'interessato; iii) responsabile della protezione dei dati e iv) registro delle attività di trattamento.

Andiamo, quindi, con ordine.

**i. Trattamento dei dati relativi alla salute in ambito sanitario**

L'Autorità Garante chiarisce che, qualora **il trattamento dei dati sanitari sia finalizzato alla cura del paziente, alcun consenso dovrà essere prestato da quest'ultimo**.

È, però, importante che il predetto trattamento - che dovrà essere eseguito da un professionista sanitario che opera in qualità di libero professionista ovvero all'interno della struttura sanitaria pubblica o privata - sia **esclusivamente finalizzato alla cura del paziente o, in alternativa, strettamente necessario alla stessa**.

Tale precisazione è molto rilevante, posto che restano esclusi tutti quei trattamenti attinenti in senso lato alla cura del paziente, come ad esempio quelli:

- connessi all'utilizzo delle app mediche per finalità diverse dalla telemedicina, oppure quando indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato accedano soggetti diversi da professionisti sanitari soggetti a segreto professionale;
- preordinati alla fidelizzazione della clientela ed effettuati da farmacie;

- effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali;
- effettuati da professionisti sanitari per finalità commerciali o elettorali;
- effettuati tramite il fascicolo sanitario elettronico (FSE).

In tutti questi casi, quindi, il titolare dovrà individuare una specifica base giuridica - consenso o altra condizione di legittimità prevista dall'art. 9 del GDPR - per rendere lecito il trattamento dei dati sanitari.
Con riferimento, invece, al FSE e al DSE per i quali è necessario il consenso dell'interessato (si vedano al riguardo le Linee Guida in tema di fascicolo sanitario elettronico e di dossier sanitario), l'Autorità Garante non esclude che in un futuro si possa rivedere tale impostazione per consentire che l'implementazione del fascicolo e del dossier sia possibile anche in assenza di consenso dell'interessato.

**ii. <u>Informazioni da fornire all'interessato</u>**

Al riguardo l'Autorità Garante non aggiunge elementi di novità, limitandosi semplicemente a ribadire che è diritto dell'interessato essere informato dal titolare circa gli elementi principali del trattamento.
Il titolare deve, quindi, rendere all'interessato tutte le informazioni in modo semplice e chiaro, scegliendo le modalità più appropriate al caso concreto.
Quanto al contenuto, invece, il Garante si sofferma unicamente sul periodo di conservazione dei dati, uno degli elementi di novità introdotti dal GDPR. In particolare, evidenzia che i tempi di conservazione della documentazione sanitaria sono molteplici e restano disciplinati da precise disposizioni normative, ad oggi in vigore. Precisa, ad esempio, che la documentazione inerente accertamenti effettuati nel corso di visite per il rilascio del certificato di idoneità all'attività sportiva agonistica deve essere conservata per cinque anni, le cartelle cliniche per un periodo illimitato e la documentazione iconografica radiologica per un periodo non inferiore a dieci anni.
In tutti quei casi, invece, in cui il periodo di conservazione non sia stabilito da una precisa disposizione normativa, il titolare è tenuto a conservare i dati per il periodo strettamente necessario al conseguimento delle finalità per le quali i dati sono trattati. Il tutto sempre nel rispetto del principio di limitazione della conservazione.

**iii. <u>Responsabile della protezione dei dati (DPO)</u>**

Fermi restando i casi di obbligatorietà della nomina del DPO espressamente sanciti dal GDPR, l'Autorità Garante ribadisce che l'adozione di tale figura è obbligatoria sia per le aziende sanitarie appartenenti al SSN, sia per gli ospedali privati, le case di cura o le residenze sanitarie assistenziali (RSA).
Ciò, in quanto se da un lato l'azienda sanitaria appartenente al SSN rientra chiaramente nella definizione di "organismo pubblico", dall'altro si configura un trattamento di dati particolari su larga scala.
Restano, quindi, esclusi dall'obbligatorietà della nomina il singolo professionista che opera in regime di libera professione a titolo individuale, le farmacie, le parafarmacie e le aziende ortoepiche e sanitarie.
A prescindere da quanto chiarito dall'Autorità Garante, preme però evidenziare che con riferimento al medico di medicina generale si sono fatte largo alcune interpretazioni, secondo cui la nomina del DPO sarebbe necessaria o comunque da valutare caso per caso.

Accade spesso, infatti, che il numero dei pazienti di un medico di medicina generale - da valutarsi anche in percentuale rispetto alla popolazione di riferimento - sia di gran lunga superiore rispetto a quello di un medico che opera in regime di libera professione a titolo individuale e potrebbe, quindi, configurarsi un "*trattamento su larga scala di categorie particolari di dati personali*", che fa scattare l'obbligo di nomina del DPO.

Ciò, a maggior ragione, in tutti i casi di esercizio della professione in forma "aggregata".

Occorre, quindi, esaminare attentamente ogni singola situazione, in modo da essere poi in grado di giustificare le scelte effettuate, così come previsto dal principio di accountability.

**iv. <u>Registro delle attività di trattamento</u>**

Ultimo aspetto analizzato, ma non per questo meno importante.

Il Garante chiarisce che l'adozione del registro delle attività di trattamento, oltre ad essere fondamentale per dimostrare il rispetto del principio di accountability, è altresì obbligatoria in ambito sanitario, essendovi trattamenti di categorie particolari di dati.

Sono, quindi, obbligati alla tenuta del registro tutti i seguenti soggetti:

- singoli professionisti sanitari che agiscono in libera professione;
- medici di medicina generale e pediatri di libera scelta;
- ospedali privati;
- case di cura;
- RSA;
- aziende sanitarie appartenenti al SSN;
- farmacie e parafarmacie e aziende ortopediche.

Seppur i predetti chiarimenti abbiamo sgombrato il campo da molti dubbi e perplessità, sono ancora numerosi gli aspetti da valutare ed esaminare in ambito sanitario. Non resta, quindi, che attendere nuovi provvedimenti da parte dell'Autorità Garante.