

Trattamento dei dati relativi alla salute in ambito sanitario: i chiarimenti del Garante per la privacy

Con il provvedimento del 7 marzo 2019, il Garante per la protezione dei dati personali ha fornito importanti chiarimenti in merito all'applicazione della disciplina di protezione dei dati in ambito sanitario, al fine di supportare tutti i soggetti operanti nel settore sanitario nel processo di attuazione di tale disciplina e di favorire un'interpretazione uniforme del nuovo assetto normativo.

L'Autorità, pur rilevando come il quadro regolatorio non sia ancora definitivo, in considerazione delle numerose segnalazioni e quesiti pervenuti relativamente ai nuovi adempimenti per i titolari e i responsabili previsti dal Regolamento e dal Codice, ha ritenuto opportuno indicare le seguenti precisazioni sull'applicazione della disciplina di protezione dei dati in ambito sanitario.

I medici potranno trattare i dati dei pazienti, per finalità di cura, senza dover richiedere il loro consenso, ma dovranno comunque fornire loro informazioni complete sull'uso dei dati. Il medico che opera come libero professionista non è tenuto a nominare il Responsabile della protezione dati. Tutti gli operatori del settore dovranno tenere un registro dei trattamenti dei dati. Questi sono i principali chiarimenti forniti dal Garante della privacy a cittadini, medici, asl e soggetti privati, sulle novità introdotte, in ambito sanitario, dal Regolamento UE in materia di protezione dei dati (GDPR) e dalla normativa nazionale.

Il provvedimento generale [n. 55 del 7 marzo 2019](#) del Garante per la privacy "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario" ha chiarito, ad esempio, che il professionista sanitario (come il medico), soggetto al segreto professionale, non deve più richiedere il consenso per i trattamenti di dati necessari alla prestazione sanitaria.

E' invece richiesto il consenso quando tali trattamenti non sono strettamente necessari per le finalità di cura, anche quando sono effettuati da professionisti della sanità, come per esempio:

- i trattamenti di dati sulla salute connessi all'uso di "App" mediche (ad eccezione di quelle per la telemedicina)
- i trattamenti di dati effettuati per la fidelizzazione della clientela (come quelli praticati da alcune farmacie o parafarmacie)
- i trattamenti di dati per finalità promozionali, commerciali o elettorali
- sulla base dell'attuale normativa che regola il settore, rimane la necessità di acquisire il consenso anche per il trattamento dei dati relativo al fascicolo sanitario elettronico, o per la consultazione dei referti online.

Il Garante fornisce chiarimenti anche in merito all'informativa agli interessati, che deve essere concisa, trasparente, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro. Rispetto alla informativa precedente al GDPR, essa deve contenere maggiori informazioni a tutela dell'interessato quali, ad esempio, quelle relative ai tempi di conservazione dei dati, che - se non sono specificati dalla normativa di settore - dovranno comunque essere individuati dal titolare (ad esempio il medico specialista o l'ospedale).

Al riguardo, si ricorda che l'ordinamento giuridico nazionale prevede numerosi e differenziati riferimenti ai tempi di conservazione della documentazione sanitaria, che non sono stati modificati dalla disciplina sulla protezione dei dati personali, ad esempio:

- documentazione inerente gli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica, che deve essere conservata, a cura del medico visitatore, per almeno cinque anni (art. 5, D.M. 18/02/1982);
- conservazione delle cartelle cliniche che, unitamente ai relativi referti, vanno conservate illimitatamente (Circolare del Ministero della Sanità del 19 dicembre 1986 n.900 2/AG454/260);
- documentazione iconografica radiologica, che deve essere conservata per un periodo non inferiore a dieci anni (art. 4, d.m. 14 febbraio 1997)

L'Autorità dedica una sezione anche al Responsabile per la protezione dei dati (RPO o DPO nell'acronimo inglese) chiarendo che:

- sono tenuti alla nomina tutti gli organismi pubblici, nonché gli operatori privati che effettuano trattamenti di dati sanitari su larga scala, quali le case di cura e le residenze sanitarie assistenziali

- non sono tenuti alla nomina i liberi professionisti sanitari che operino in regime di libera professione a titolo individuale o altri soggetti, come le farmacie, che non effettuano trattamenti su larga scala.

Il Garante non specifica il caso dello studio associato, per il quale si ritiene che il discrimine sia la larga scala del trattamento.

Il Garante infine chiarisce che è obbligatorio tenere il registro delle attività di trattamento effettuate sui dati dei pazienti per tutti gli operatori sanitari: i singoli professionisti sanitari che agiscano in libera professione, i medici di medicina generale/pediatri di libera scelta (MMG/PLS), gli ospedali privati, le case di cura, le RSA e le aziende sanitarie appartenenti al SSN, nonché le farmacie, le parafarmacie e le aziende ortopediche. Tale documento rappresenta, in ogni caso, un elemento essenziale per il “governo dei trattamenti” e per l’efficace individuazione di quelli a maggior rischio, anche per dimostrare il rispetto del principio di responsabilizzazione (accountability) previsto dal GDPR.

Fonte: Garante Privacy