GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 [9091942]

VEDI ANCHE: Newsletter del 25 marzo 2019

[doc. web n. 9091942]

Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019

Registro dei provvedimenti
n. 55 del 7 marzo 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle

persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati di seguito Regolamento);

VISTO il d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTI gli artt. 57, par. 1, lett. b) e d) del Regolamento e 154, comma 1, lett. g) del Codice in merito al compito attribuito al Garante di promuovere la consapevolezza e di favorire la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione ai trattamenti, nonché agli obblighi imposti ai titolari e i responsabili del trattamento;

VISTO il Considerando n. 132 del Regolamento che prevede attività di sensibilizzazione delle autorità di controllo nei confronti del pubblico;

VISTE le Faq sul Responsabile della Protezione dei Dati (RPD) in ambito pubblico e privato pubblicate su www.gpdp.it (doc. web nn. 7322110 e 8036793);

VISTE le Faq sul Registro delle attività di trattamento pubblicate su www.gpdp.it (doc. web n. 9047529);

ESAMINATE le segnalazioni e i quesiti pervenuti in ordine al trattamento dei dati personali in ambito sanitario, relativi ai nuovi adempimenti per i titolari e i responsabili previsti dal Regolamento e dal Codice;

ESAMINATE, altresì, le segnalazioni e i quesiti che evidenziano dubbi interpretativi derivanti dal mutato e articolato assetto della disciplina relativa al trattamento dei dati relativi alla salute nel settore sanitario;

CONSIDERATO che le segnalazioni e i quesiti pongono problematiche comuni che vanno opportunamente esaminate congiuntamente;

RITENUTA l'opportunità di supportare tutti i soggetti operanti in ambito sanitario nel processo di attuazione della richiamata disciplina, nonché di favorire un'interpretazione uniforme del nuovo assetto normativo, fornendo orientamenti utili per i cittadini e gli operatori del settore, con particolare riferimento ai responsabili della protezione dei dati;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Antonello Soro;

PREMESSA

Il trattamento dei dati sulla salute è consentito in presenza di taluni requisiti specifici individuati all'art. 9 del Regolamento (cfr. considerando n. 51), il quale ha previsto, in questo ambito, la possibilità per gli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riferimento al predetto trattamento (cfr. art. 9, par. 4). Il decreto legislativo n. 101/2018, in vigore dal 19 settembre 2018, ha previsto, al riguardo, che il Garante completi l'individuazione dei presupposti di liceità dei suddetti trattamenti, adottando specifiche misure di garanzia e promuovendo l'adozione di regole deontologiche (artt. 2-septies e 2-quater del Codice).

Considerata la delicatezza e la complessità di tali trattamenti, il legislatore ha, inoltre, previsto un periodo transitorio, affidando al Garante il compito di individuare, ed eventualmente aggiornare, le prescrizioni contenute nelle autorizzazioni generali sul trattamento dei dati sensibili che risultavano compatibili con le disposizioni del Regolamento e del decreto n. 101/2018, nonché di verificare la conformità dei codici deontologici al Regolamento (artt. 20 e 21 del citato decreto).

In attuazione della predetta disciplina transitoria, con il provvedimento del 13 dicembre 2018 (consultabile sul sito www.gpdp.it,

doc. web n. 9068972), sono state individuate le prescrizioni, contenute nelle autorizzazioni generali, compatibili con le disposizioni del Regolamento e del decreto n. 101/2018, deliberando contestualmente l'avvio di una procedura di consultazione pubblica, al fine di acquisire osservazioni e proposte a cura di tutti i soggetti interessati.

Analogamente, con provvedimento del 19 dicembre 2018 (doc. web n.9069637), il Garante ha provveduto alla verifica della conformità delle disposizioni contenute nei Codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, statistici, scientifici al Regolamento e alla loro conversione in regole deontologiche, il cui rispetto costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali (art. 2-quater del Codice).

L'Autorità ha, altresì, avviato la redazione dei provvedimenti, previsti dall'art. 2-septies del Codice, che stabiliscono le misure di garanzia e si impegna ad adottarli in tempi brevi per arrivare, quanto prima, alla completa definizione del quadro regolatorio.

In questi primi mesi di applicazione del Regolamento e delle nuove disposizioni del Codice, il Garante ha ricevuto numerosi quesiti in ordine al nuovo assetto della disciplina relativa al trattamento dei dati relativi alla salute in ambito sanitario.

E' stata sollevata, infatti, in più occasioni, l'esigenza, da parte degli operatori del settore, dei soggetti istituzionali competenti, dei responsabili della protezione dati e dei cittadini di avere dei chiarimenti in merito al mutato e articolato assetto della disciplina in tale ambito.

Sebbene il quadro regolatorio, come sopra evidenziato, non sia ancora definitivo, l'Autorità ritiene opportuno fornire alcuni chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario.

1. Disciplina per il trattamento dei dati relativi alla salute in ambito sanitario

Le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per:

a. **motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;

b. **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c. **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

Ciò non esclude che a seconda dello specifico trattamento effettuato, non possa ritenersi applicabile al caso concreto una delle altre deroghe previste dall'art. 9 del Regolamento.

In proposito, si osserva che la fattispecie indicata alla c) del precedente elenco presenta alcune peculiarità che ne caratterizzano l'applicabilità. Al riguardo, si precisa, innanzitutto, che i trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2, lett. h) e par. 3 del Regolamento, sono propriamente quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza. Diversamente dal passato, quindi, il professionista sanitario, soggetto al segreto professionale, non deve più richiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dalla circostanza che operi in qualità di libero professionista (presso uno studio medico) ovvero all'interno di una struttura sanitaria pubblica o privata.

Altro aspetto riguarda l'ambito oggettivo: i trattamenti di cui all'art. 9, par. 2, lett. h) sono infatti quelli "necessari" al perseguimento

delle specifiche “finalità di cura” previste dalla norma, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (cfr. considerando 53 del Regolamento).

Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell’interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento).

Con riferimento ai trattamenti in ambito sanitario che non rientrano nelle ipotesi sopra descritte e, quindi, che richiedono il consenso esplicito dell’interessato (art. 9, par. 2, lett. a) del Regolamento), si individuano, a titolo esemplificativo, le seguenti categorie:

a. trattamenti connessi all’utilizzo di **App mediche**, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell’interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell’applicazione, ai dati dell’interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale (cfr. Faq CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità(1));

b. trattamenti preordinati alla **fidelizzazione della cliente**la, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell’ambito del Servizio sanitario nazionale (SSN);

c. trattamenti effettuati in campo sanitario da **persone giuridiche private per finalità promozionali o commerciali** (es. promozioni su programmi di screening, contratto di fornitura di servizi ammnistrativi, come quelli alberghieri di degenza);

d. trattamenti effettuati da professionisti sanitari per **finalità commerciali o elettorali** (cfr. provv. del 6 marzo 2014, doc. web n. 3013267);

e. trattamenti effettuati attraverso il **Fascicolo sanitario elettronico** (d.l. 18 ottobre 2012, n. 179, art. 12, comma 5) In tali casi, l’acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore, precedenti all’applicazione del Regolamento, il cui rispetto è ora espressamente previsto dall’art. 75 del Codice. Al riguardo, un’eventuale opera di rimeditazione normativa in ordine all’eliminazione della necessità di acquisire il consenso dell’interessato all’alimentazione del Fascicolo, potrebbe essere ammissibile alla luce del nuovo quadro giuridico in materia di protezione dei dati.

Con riferimento ai trattamenti effettuati attraverso il Dossier sanitario, il consenso è attualmente richiesto dalle Linee guida emanate dall’Autorità prima dell’applicazione del Regolamento (Linee guida in materia di Dossier sanitario del 4 giugno 2015, doc web. n. 4084632). Alla luce del nuovo quadro giuridico, sarà il Garante ad individuare, nell’ambito delle misure di garanzia da adottarsi sulla base dell’art. 2-septies del Codice, i trattamenti che, ai sensi dell’art. 9, par. 2, lett. h), possono essere effettuati senza il consenso dell’interessato.

Diverso è il caso della refertazione on line per il quale il consenso dell’interessato è richiesto dalle disposizioni di settore in relazione alle modalità di consegna del referto (Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013, art. 5).

In conclusione, occorre evidenziare che, così come richiamato dall’art. 22, comma 1, del d.lgs. n. 101/2018, le disposizioni del Codice si devono, in ogni caso, interpretare e applicare alla luce del Regolamento.

2. Informazioni da fornire all’interessato

Il principio di trasparenza previsto dall’art. 5, par. 1, lett. a) del Regolamento impone ai titolari di informare l’interessato sui principali elementi del trattamento, al fine di renderli consapevoli sulle principali caratteristiche dello stesso.

Al riguardo, si rappresenta che, pur nel rispetto dell’obbligo di comunicare gli elementi di cui agli artt. 13 e 14 del Regolamento, le informazioni da rendere all’interessato vanno rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro (cfr. art. 12, par. 1, del Regolamento, e art. 78 del Codice). Riguardo alle modalità con cui fornire l’informativa, alla luce del principio di responsabilizzazione di cui all’art. 5 del Regolamento, spetta al titolare scegliere le modalità

più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato (ad esempio, il dispositivo utilizzato, la natura dell'interazione con il titolare e le eventuali limitazioni che implicano tali fattori; cfr. considerando nn. 58 e 60) (2).

Relativamente al contenuto, il Regolamento non stravolge l'impianto delle informazioni da rendere all'interessato, ma prevede solo alcuni nuovi elementi informativi rispetto a quanto era previsto nell'art. 13 del Codice. Pertanto, l'informativa, predisposta in passato dai titolari dovrebbe essere aggiornata e integrata solo con riferimento agli elementi di novità previsti dagli artt. 13 e 14 del Regolamento.

Con specifico riferimento all'attività posta in essere da titolari del trattamento operanti in ambito sanitario che effettuano una pluralità di operazioni connotate da particolare complessità (es. aziende sanitarie), si ritiene opportuno suggerire di fornire all'interessato le informazioni previste dal Regolamento in modo progressivo. Ciò significa che nei confronti della generalità dei pazienti afferenti a una struttura sanitaria potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie (cfr. art. 79 del Codice). Gli elementi informativi relativi a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici on-line, finalità di ricerca) potrebbero essere resi, infatti, in un secondo momento, solo ai pazienti effettivamente interessati da tali servizi e ulteriori trattamenti. Ciò andrebbe a beneficio di una maggiore attenzione alle informazioni veramente rilevanti, fornendo la piena consapevolezza circa gli aspetti più significativi del trattamento.

Tra gli elementi informativi di novità, merita evidenziare quello relativo al periodo di conservazione dei dati che, secondo il Regolamento, può essere fornito dal titolare anche attraverso l'indicazione dei criteri utilizzati per determinarlo (artt. 13 e 14, par. 2, lett. a), Regolamento).

Al riguardo, si ricorda che, con particolare riferimento alla documentazione sanitaria, l'ordinamento giuridico prevede numerosi e differenziati riferimenti ai tempi di conservazione della stessa, che non sono stati modificati dalla disciplina sulla protezione dei dati personali e che, quindi, rimangono pienamente in vigore. Si fa riferimento, ad esempio: alla 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); alla 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); alla documentazione iconografica radiologica, che deve essere conservata per un periodo non inferiore a dieci anni (art. 4, d.m. 14 febbraio 1997).

Nel caso in cui, invece, i tempi di conservazione di specifici documenti sanitari non siano stabiliti da una disposizione normativa, il titolare del trattamento, in virtù del principio di responsabilizzazione, dovrà individuare tale periodo in modo che i dati siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati (principio di limitazione della conservazione, art. 5, par. 1, lett. e) del Regolamento) e indicare tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato.

3. Responsabile della protezione dei dati (RPD)

La designazione del RPD nella struttura del Regolamento costituisce una misura volta a facilitare l'osservanza della disciplina di protezione dei dati, che risulta obbligatoria per le autorità o organismi pubblici; per gli altri soggetti tale obbligo sussiste invece solo al ricorrere delle specifiche condizioni di cui all'art. 37.

In generale, si ritiene che i trattamenti dei dati personali relativi a pazienti effettuati da un'azienda sanitaria appartenente al SSN devono essere ricondotti a quelli per i quali è prevista la designazione obbligatoria del RPD, sia in relazione alla natura giuridica di "organismo pubblico" del titolare, sia in quanto rientrano nella condizione prevista dall'art. 37, par. 1, lett. c), considerato che le attività principali del titolare consistono nel trattamento, su larga scala, di dati sulla salute.

Si ritiene che anche il trattamento dei dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da una residenza sanitaria assistenziale (RSA) possa rientrare, in linea generale, nel concetto di larga scala. (Linee guida sui Responsabili della protezione dei dati, WP243, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, punto 2.1.3, doc. web n. 612048, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, cfr. Endorsement n. 1/2018).

Anche per gli aspetti organizzativi dell'ufficio del RPD, la possibilità e la fattibilità (art. 39 del Regolamento) di nominare un unico

RPD per più strutture sanitarie, è rimessa alla responsabilità del titolare del trattamento.

Quanto, poi, al singolo professionista sanitario che operi in regime di libera professione a titolo individuale, si fa presente che lo stesso non è tenuto alla designazione di tale figura con riferimento allo svolgimento della propria attività.

Secondo quanto indicato nel Considerando n. 91 del Regolamento, infatti, i trattamenti dallo stesso effettuati non rientrano tra quelli su larga scala. In tal senso, anche il Gruppo di lavoro Art. 29 per la protezione dei dati (ora Comitato europeo per la protezione dei dati-art. 68 del Regolamento) indica, tra gli esempi di trattamento da non considerare su larga scala, quelli svolti da un singolo professionista sanitario (Linee guida sui Responsabili della protezione dei dati, cit., punto 2.1.3.).

Analoghe considerazioni valgono anche per le farmacie, le parafarmacie, le aziende ortopediche e sanitarie. Pertanto, i citati soggetti, se non effettuano trattamenti di dati personali su larga scala, non sono obbligati a designare il RPD.

4. Registro delle attività di trattamento

I registri delle attività di trattamento rappresentano uno degli elementi per la definizione del quadro generale di accountability previsto dal Regolamento. Per dimostrare di conformarsi a tale disciplina, infatti, il titolare/il responsabile devono tenere un registro delle attività di trattamento effettuate sotto la loro responsabilità (cfr. Considerando n. 82). La tenuta del registro costituisce un elemento essenziale per il governo dei trattamenti e per l'efficace individuazione di quelli a maggior rischio.

Con riferimento a questo adempimento si rappresenta, in linea generale, la sussistenza di tale obbligo in ambito sanitario. Tale posizione tiene conto del fatto che, essendo le fattispecie di esenzione di cui all'art. 30, par. 5 del Regolamento tra loro alternative (cfr. Gruppo di lavoro Art. 29 per la protezione dei dati - Position paper related to article 30(5), fatte proprie dal Comitato europeo per la protezione dei dati-Endorsement n. 1/2018), la deroga alla tenuta del registro non opera in presenza anche di uno solo degli elementi indicati dal predetto par. 5 (trattamento che presenta un rischio per i diritti e le libertà per l'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati). Ciò, in coerenza con la circostanza che il registro delle attività del trattamento costituisce uno strumento di accountability e di gestione del rischio.

Per le suddette ragioni, si ritiene, quindi, che non ricadono nelle ipotesi di esenzione dall'obbligo di tenuta del registro 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.

In merito alla tenuta del registro delle attività di trattamento, si precisa, infine, che lo stesso non deve essere trasmesso al Garante, ma messo a disposizione dell'Autorità in caso di controllo.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 57, par. 1, lett. b) e d) del Regolamento e 154, comma 1, lett. g) del Codice, adotta il presente provvedimento.

Roma, 7 marzo 2019

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

———————

(1) Faq della Commission Nationale de l'Informatique et des Libertés del 17 luglio 2018, in https://www.cnil.fr/fr/applications-mobiles-en-sante-et-protection-des-donnees-personnelles-les-questions-se-poser

(2) Cfr., altresì, le Linee guida sulla trasparenza ai sensi del Regolamento, WP260, adottate il 29 novembre 2017, versione emendata l'11 aprile 2018, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (Endorsement n. 1/2018).