GPDP.Ufficio.PROTOCOLLO.U.0014338.17-05-2016.h.10:48

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

IL PRESIDENTE

Gentilissima Presidente

facendo seguito alla Sua nota del 22 aprile u.s., nell'ottica della collaborazione che caratterizza il rapporto tra l'Autorità e le associazioni di categoria, l'Ufficio ha predisposto l'allegato documento riportante sintetici elementi di risposta ai quesiti sottoposti, con l'intento di chiarire quanto previsto dalla disciplina in materia di protezione dati personali e da alcuni provvedimenti adottati dall'Autorità sul trattamento dati in ambito sanitario.

Cordiali saluti

Antonello Soro

Dott.ssa Roberta Chersevani
Presidente
FNOMCeO
Piazza Cola di Rienzo, 80/a
00192 Roma

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696772312/3 - Fax +39 06 696773315
a.soro@gpdp.it
www.garanteprivacy.it

RISPOSTE AI QUESITI DELLA FNOMCEO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

1. Secondo le norme del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 - di seguito Codice) il consenso al trattamento dei dati idonei a rivelare lo stato di salute può essere manifestato anche oralmente. In tal caso, il consenso è documentato, anziché con atto scritto dell'interessato (firma), con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico anche mediante annotazione su un sistema informatico.

Restano, ovviamente, ferme le disposizioni relative all'efficacia probatoria di scritti e dichiarazioni.

Con specifico riferimento al FSE si evidenzia che l'articolo 12 del decreto-legge n. 179/2012 – successivamente modificato e integrato dall'articolo 17 del predetto decreto-legge n. 69/2013 – prevede l'istituzione, da parte delle regioni e delle province autonome, del fascicolo sanitario elettronico (FSE), definito dalla legge "*l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito*" (art. 12, comma 1, d.l. n. 179/2012).

Tale norma stabilisce che il FSE possa essere alimentato esclusivamente sulla base del consenso libero e informato dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo.

Tale consenso può essere acquisito con le modalità previste dal Codice sopra richiamate.

2. Il trattamento dei dati personali in ambito sanitario effettuato per fini di cura della salute si fonda sul binomio: consenso dell'interessato e autorizzazione del Garante (cfr. autorizzazioni generali pubblicate sul sito www.gpdp.it). Tali regole operano con riferimento ai trattamenti effettuati da parte di tutti gli esercenti le professioni sanitarie sia pubblici che privati.

Si può, tuttavia, prescindere dal richiedere un immediato consenso dell'interessato (salvo la necessita di richiederlo senza ritardo successivamente alla prestazione) nei seguenti casi:

- emergenza sanitaria o igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'art. 117 del d.lgs. n. 112/1998;
- impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;
- rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato;
- prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia (art. 82 del Codice).

Piazza di Monte Citorio, 121 · 00186 Roma
Tel. +39 06 696772312/3 - Fax +39 06 696773315
a.soro@gpdp.it
www.garanteprivacy.it

Si può anche prescindere dal consenso dell'interessato, purché si rispetti l'autorizzazione n. 2 del Garante, per porre in essere un trattamento finalizzato alla tutela della salute o dell'incolumità fisica di un terzo o della collettività (art. 76 del Codice).

Una disciplina speciale è invece dettata per il trattamento di dati personali da parte dei soggetti pubblici per finalità di carattere amministrativo strettamente correlate alla cura della salute. Tali trattamenti non si fondano sul consenso dell'interessato, bensì sul rispetto della quadro normativo di settore in cui siano specificati i tipi di dati che possono essere trattati e di operazioni eseguibili, nonché le finalità di rilevante interesse pubblico perseguite (art. 20 del Codice).

Al riguardo, la Conferenza delle regioni e delle province autonome ha redatto uno schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome e di altri soggetti fra i quali le aziende sanitarie, su cui il Garante ha già espresso parere favorevole (Provv. 13 aprile 2006, consultabile sul sito www.gpdp.it, doc. web n. 1272225). Successivamente, il Garante ha reso parere favorevole su una versione aggiornata del predetto schema tipo di regolamento in relazione alla necessità, evidenziata da parte di più enti, di adeguare i regolamenti regionali sul trattamento dei dati sensibili e giudiziari al mutato quadro normativo (cfr. Provv. 26 luglio 2012, doc. web n. 1915390).

L'allegato B) a tale schema tipo di regolamento riguarda i trattamenti di dati personali sensibili effettuati dalle strutture sanitarie pubbliche per finalità amministrative correlate alla cura dell'interessato.

Analogamente il professionista sanitario, in qualità di titolare del trattamento, non dovrà richiedere il consenso dell'interessato per trattare i dati personali del paziente che si rilevino indispensabili per assolvere ad un obbligo previsto da una norma di legge e di regolamento (es. denuncia obbligatoria in caso di rilevazione di particolari malattie).

3. Con riferimento a tale domanda è bene distinguere i casi in cui il professionista (titolare) comunichi ad un soggetto pubblico (autonomo titolare) dati personali del paziente in assolvimento a un obbligo legislativo, dal caso in cui tale comunicazione avvenga verso soggetti terzi privati a cui il professionista stesso abbia delegato -tramite contratto- funzioni proprie (es. conservazione dei dati) (c.d. *outsourcing*).

Nel primo caso, si tratta di una comunicazione fra due titolari autonomi del trattamento effettuata in base ad una disposizione di legge (art. 20 del Codice). In tal caso, il professionista sanitario deve comunicare i dati personali nel rispetto delle misure di sicurezza, limitando l'invio ai soli dati indispensabili ad assolvere all'obbligo di legge. Sarà cura, poi, del soggetto che li riceve trattare tali dati per le finalità ad esso attribuite dalla legge e nel rispetto delle disposizioni vigenti.

Nel caso in cui il professionista (titolare) decida di avvalersi di un soggetto esterno per lo svolgimento di alcune funzioni ad esso imputabili è necessario che designi tale soggetto responsabile del trattamento (*outsourcer*) e mantenga nei suoi riguardi specifici compiti di vigilanza (art. 28 e 29 del Codice). In questo caso, infatti, il terzo destinatario del dato non assume la qualifica di titolare ed è tenuto, in quanto responsabile esterno, a rispettare le istruzioni del titolare e a operare nei limiti indicati nella relativa designazione.

4. Preliminarmente occorre rilevare che non sussistono ad oggi specifiche disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni con riguardo sia all'*an* sia al *quantum*. Di volta in volta, infatti, l'intervento dell'Autorità si è reso necessario per colmare tale vuoto, attraverso la prescrizione in diversi ambiti di tale misure (cfr. Provv. 21 ottobre 2009, doc. web n. 1683093; Provv. 18 settembre 2008, doc. web n. 1549548; Provv. 12 maggio 2011, doc. web n. 1813953; Provv. 4 giugno 2015, doc. web n. 4084632). Solo in alcuni casi, inoltre, il Garante ha ritenuto necessario prescrivere espressamente anche la misura circa l'immodificabilità dei *log* anche in considerazione della particolare complessità della stessa.

Le specifiche prescrizioni rese dal Garante con riferimento ai trattamenti effettuati tramite il dossier sanitario, anche con riferimento alla tracciabilità degli accessi al dossier (Provv. 4 giugno 2015, doc. web n. 4084632), nasce dalla particolare delicatezza dei dati personali trattati in questo ambito; ciò impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).

In tal senso, le strutture sanitarie, nell'ambito della discrezionalità riconosciuta nell'organizzare la funzione di *compliance*, devono realizzare sistemi di controllo delle operazioni effettuate sui sistemi informativi in uso, mediante procedure che prevedano la registrazione automatica in appositi file di *log* degli accessi e delle operazioni compiute.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati sanitari dei pazienti. Tale attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere comunicato alle persone e agli organi legittimati ad adottare decisioni e messo a disposizione del Garante, in caso di specifica richiesta (cfr., in tal senso, citate Linee guida in materia di dossier sanitario del 4 giugno 2015).

5. Non sussistono, allo stato, specifici impedimenti normativi alla tenuta delle grandi banche dati pubbliche presso soggetti aventi sede in Paesi siti fuori dall'Unione europea. In tali casi resta ovviamente fermo il necessario rispetto delle disposizioni del Codice con particolare riferimento a quelle relative al trasferimento dei dati all'estero (artt.42 e 43 del Codice).

Il legislatore, infatti, non ha ancora fissato specifiche regole per la gestione delle grandi banche dati pubbliche anche se, al riguardo, sussiste un vivace dibattito parlamentare. Il tema delle grandi banche dati è sempre stato centrale per l'attività dell'Autorità, come dimostrano i numerosi interventi in materia nei confronti del Ministero della salute, di Sogei e dell'Inps e, da ultimo, il provvedimento sulle misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche del 2 luglio 2015.

Si evidenzia, infine, che tra i compiti demandati dal legislatore all'Autorità vi è anche quello di vigilanza sul rispetto del quadro normativo vigente in materia di protezione dei dati personali.

6. Tutti i soggetti che accedono ai dati personali all'interno della struttura sanitaria devono essere designati responsabili o incaricati del trattamento. Nell'ambito della relativa designazione saranno indicate loro le specifiche operazioni che possono compiere sui dati personali (artt. 28, 29 e 30 del Codice).

Con specifico riferimento al personale amministrativo operante all'interno della struttura sanitaria, lo stesso, in qualità di incaricato del trattamento, può consultare le informazioni indispensabili per assolvere alle funzioni amministrative cui è preposto (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche può trattare i dati indispensabili per la prenotazione stessa). Fermo restando, quindi, che il personale di una struttura sanitaria deve poter accedere al minimo di informazioni necessarie per lo svolgimento delle proprie funzioni, ivi comprese anche, nel contesto sanitario, le informazioni idonee a rivelare lo stato di salute, è preciso compito e responsabilità della struttura sanitaria adottare tutte le misure idonee per prevenire i rischi di accesso non autorizzato o trattamento non consentito o non conforme (art. 31 del Codice). In questo senso, un adeguato processo di designazione degli incaricati, di conferimento di istruzioni e un congiunto sistema di autorizzazione informatica (regole 12-14, allegato B) al Codice) costituiscono la migliore garanzia di *compliance*.

Con specifico riferimento al sospetto diagnostico, si evidenzia che specifiche disposizioni normative indicano i casi in cui lo stesso debba essere apposto nella prescrizione medica (ad es., d.P.R. 28/07/2000, n. 270).

In linea più generale, l'analisi circa la profondità degli accessi ai dati personali dei pazienti deve essere effettuata anche con riferimento al personale sanitario, al fine di valutare se sia sempre necessario consentire l'accesso a tutti i dati trattati dalla struttura sanitaria (artt. 11, comma 1, lett. d) e 22, comma 5, del Codice).

Devono essere, pertanto, preferite soluzioni che consentano un'organizzazione modulare dei sistemi informativi utilizzati, in modo tale da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili al raggiungimento dello scopo per il quale è stato consentito l'accesso.

Con specifico riferimento alla prestazione del consenso dell'interessato, si richiama, infine, quanto indicato nel precedente punto 2 con riferimento ai trattamenti effettuati per fini amministrativi correlati alla cura.

7. Non sussistono nel nostro ordinamento giuridico ipotesi di esenzione come quelle rappresentate; non rientra, inoltre, tra i compiti dell'Autorità prevederle.

8. Il Codice in materia di protezione dei dati personali prevede un sistema di manifestazione della volontà dell'interessato fondato sul c.d. *opt-in*; il consenso, pertanto, deve essere espresso, non potendo desumersi lo stesso da un comportamento concludente dell'interessato.

In ambito sanitario è stata prevista una forma di semplificazione con riferimento alla possibilità di acquisire tale consenso oralmente, purché vi sia una sua documentazione per iscritto (cfr. precedente punto 2).

L'invio dei dati personali dei soggetti che hanno usufruito di una prestazione sanitaria ai fini dell'elaborazione del 730, è stato espressamente previsto dalla normativa di settore. Trattandosi di un trattamento in ambito pubblico il presupposto

di liceità è da individuarsi, pertanto, nella norma di legge di riferimento e non nel consenso dell'interessato; il dissenso all'invio costituisce una modalità di opposizione contemplata da tale quadro normativo. È bene evidenziare che l'invio dei suddetti dati non è finalizzato alla cura, bensì alla predisposizione da parte dell'amministrazione finanziaria di uno strumento per facilitare il cittadino negli adempimenti fiscali.

9. Le responsabilità in merito al trattamento dei dati personali disciplinate dal Codice costituiscono fattispecie diverse da quelle relative al rischio professionale. A tali forme di responsabilità si applicano gli istituti amministrativi, civili e penali previsti dalle legge.

In ciascuno dei tre diversi ambiti i criteri di imputazione delle responsabilità seguono pertanto regole specifiche definite dal Codice civile, penale e dalle disposizioni sul procedimento sanzionatorio (l. n. 689/1981), nonché dal Codice in materia di protezione dei dati personali. La logica di fondo è semmai opposta: ognuno risponde, in diverse sedi e a diverso titolo, degli eventi che con le proprie azioni o omissioni (per colpa o per dolo) ha contribuito a causare.

10. Con riferimento al primo quesito relativo alla possibilità per gli Ordini dei Medici Chirurghi e degli Odontoiatri di *"pubblicare sul proprio albo online l'informazione sulla regolarità formativa del professionista"* si osserva preliminarmente che il Codice dispone che i soggetti pubblici possono comunicare a soggetti terzi o diffondere dati personali, diversi da quelli sensibili e giudiziari, solo se tali specifiche operazioni di trattamento risultano ammesse da una norma di legge o di regolamento (artt. 4, comma 1, lett. b), c), d), e), l) e m), 19, comma 3). Per il trattamento di dati personali da parte di soggetti privati il Codice individua, invece, come presupposto di liceità il consenso dell'interessato ovvero specifici presupposti ad esso equipollenti tra i quali rileva, in particolare, la necessità di adempiere ad una norma di legge o di regolamento (art. 23, comma 1, e 24, comma 1, lett. a), del Codice).

In tale quadro, il successivo articolo 61 (commi 2, 3 e 4) dispone che:

"(...) i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari".

Ciò premesso, allo stato della normativa vigente, in assenza di una norma di legge o di regolamento che espressamente preveda l'inserimento nell'albo dell'informazione relativa alla c.d. regolarità formativa dei professionisti, gli Ordini professionali possono evidenziare nei predetti albi tale ulteriore informazione solo su esplicita richiesta dell'interessato, potendosi certamente ritenere che tale dato soddisfi

le richiamate caratteristiche di pertinenza e non eccedenza rispetto all'attività professionale svolta (art. 61, comma 2, del Codice). Ciò, tenuto anche conto che, in base alla specifica disciplina di settore, la violazione dell'obbligo di formazione continua determina un illecito disciplinare (art. 3, comma 5, lett. b), del d.l. 13 agosto 2011, n. 138, convertito con modificazioni in legge 14 settembre 2011, n. 148).

In relazione, al secondo quesito relativo alla possibilità per il "Consorzio gestione anagrafica delle professioni sanitarie" (Co.Ge.A.P.S.) di consentire ad altri enti pubblici la visualizzazione dei dati di dettaglio sulla formazione continua per la verifica della regolarità formativa del professionista, nel richiamare il predetto quadro normativo, si evidenzia, che non risulta allo stato possibile per il Co.Ge.A.P.S. consentire ad altri enti pubblici la visualizzazione dei dati di dettaglio sulla formazione continua per la verifica della regolarità formativa del professionista. Ciò, anche in considerazione del fatto che lo statuto stesso del Co.Ge.A.P.S. prevede che "*è espressamente vietato al Consorzio acquisire o vantare o cedere a terzi diritti di proprietà o di uso autonomo di tali dati al di fuori del perseguimento degli scopi consortili*" che concernono esclusivamente la gestione dell'Anagrafe Nazionale dei crediti formativi ECM, nonché attività di studio e reperimento di fondi ed infrastrutture utili allo scopo della formazione continua (art. 2).