All. n. 1

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVVEDIMENTO 4 giugno 2015

Linee guida in materia di Dossier sanitario. (Provvedimento n. 331). (15A05443)

(GU n.164 del 17-7-2015)

IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito «Codice»);

Visto il «Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (Cce)» adottato il 15 febbraio 2007 dal Gruppo che riunisce le autorita' garanti di protezione dei dati (cd. Gruppo Art. 29);

Viste le «Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario» adottate dal Garante con provvedimento del 16 luglio 2009 (Gazzetta Ufficiale n. 178 del 3 agosto 2009, consultabili sul sito www.gpdp.it, doc. web n. 1634116);

Visto l'art. 12 (Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario) del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, e dall'art. 13, comma 2-quater, del decreto-legge 21 giugno 2013, n. 69, convertito dalla legge 9 agosto 2013, n. 98;

Visto il parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico del 22 maggio 2014 (doc. web n. 3230826);

Viste le segnalazioni ricevute concernenti i sistemi informativi di archiviazione e refertazione delle prestazioni sanitarie erogate, utilizzati da numerose strutture sanitarie private e del Servizio sanitario nazionale (SSN);

Viste le richieste di informazioni in atti;

Visto il provvedimento del Garante del 10 gennaio 2013 nei confronti dell'Azienda ospedaliero-universitaria Ospedali Riuniti di Trieste e delle altre aziende sanitarie della regione Friuli Venezia Giulia (doc. web n. 2284708);

Visto il provvedimento del Garante del 3 luglio 2014 nei confronti dell'Azienda sanitaria dell'Alto Adige (doc. web n. 3325808);

Visto il provvedimento del Garante del 23 ottobre 2014 nei confronti dell'Azienda ospedaliero-universitaria S. Orsola Malpighi di Bologna (doc. web n. 3570631);

Visto il provvedimento del Garante del 18 dicembre 2014 nei confronti dell'Azienda Policlinico Umberto I di Roma (doc. web n. 3725976);

Visti gli atti degli accertamenti ispettivi effettuati dall'Ufficio presso alcune aziende sanitarie del Servizio Sanitario Nazionale in merito al trattamento dei dati personali effettuato attraverso i dossier sanitari aziendali;

Considerato che negli ultimi anni le strutture sanitarie hanno notevolmente incrementato l'utilizzo di sistemi informativi per la gestione della documentazione sanitaria;

Ritenuta l'opportunita' di rendere disponibile un quadro unitario di misure e accorgimenti per conformare i trattamenti di dati personali e, in particolare, quelli idonei a rivelare lo stato di salute, alla vigente disciplina sulla protezione dei dati personali che tenga conto dell'esperienza maturata e dell'evoluzione normativa rispetto alle richiamate Linee guida del 2009;

Ritenuto, in ragione della particolare delicatezza dei dati idonei a rivelare lo stato di salute, degli specifici rischi di accesso non autorizzato e di trattamento non consentito, nonche' dell'esigenza di garantire l'esattezza, l'integrita' e la disponibilita' dei dati, di dovere assoggettare il trattamento dei dati personali effettuato attraverso il dossier a un regime generale di obbligatoria comunicazione delle eventuali violazioni;

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

Relatore la prof.ssa Licia Califano;

Premessa

Sin dal 2009 il Garante aveva avvertito l'esigenza di delineare specifiche garanzie, responsabilita' e diritti in ordine alla condivisione da parte di distinti titolari del trattamento ovvero da parte di tutti i professionisti sanitari operanti presso il medesimo titolare delle informazioni sanitarie che ricostruiscono la storia sanitaria di un individuo. In tal senso, sono state adottate le «Linee guida in tema di Fascicolo sanitario elettronico (Fse)e di dossier sanitario» (provv. del 16 luglio 2009 citato).

Successivamente, il legislatore con il richiamato d.l. 18 ottobre 2012, n. 179 (ulteriori misure urgenti per la crescita del Paese), convertito in legge 17 dicembre 2012, n. 221, ha per la prima volta dotato il nostro ordinamento giuridico di una definizione e di una disciplina normativa del Fascicolo sanitario elettronico (di seguito Fse) (art. 12). L'impianto normativo fornisce una definizione del Fse, corrispondente a quella elaborata dall'Autorita' nel 2009, ed individua quale presupposto legittimante l'utilizzo del Fascicolo il consenso al trattamento dei dati personali da parte dell'interessato, cosi' come indicato anche dal Garante nelle predette Linee guida.

Con riferimento all'assetto normativo introdotto nel 2012 in materia di Fse, l'Autorita' ha partecipato al tavolo di lavoro istituito al riguardo presso il Ministero della salute che aveva come scopo istituzionale quello di redigere una bozza di decreto di attuazione della norma primaria sul Fse, elaborando in quella sede numerose osservazioni.

In considerazione dell'accoglimento di tutte le indicazioni rese dall'Autorita', il Garante ha potuto cosi' esprimere parere favorevole sullo schema di decreto in materia di Fse (parere del 22 maggio 2014 citato).

La medesima attenzione che e' stata posta dal Garante in ordine agli aspetti di protezione dati personali connessi all'istituzione del Fascicolo sanitario elettronico e' stata rivolta anche con riferimento ai trattamenti di dati personali effettuati dalle strutture sanitarie mediante il dossier.

Secondo la definizione resa nelle citate Linee guida del 2009 il dossier sanitario e' lo strumento costituito presso un organismo sanitario in qualita' di unico titolare del trattamento (es., ospedale, azienda sanitaria, casa di cura) al cui interno operino

piu' professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es., referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica.

Il dossier sanitario, dunque, raccoglie le informazioni relative agli eventi clinici occorsi all'interessato esclusivamente presso un'unica struttura sanitaria. In via principale, pertanto, si differenzia dal Fse per la circostanza che i documenti e le informazioni sanitarie accessibili tramite tale strumento sono state generate da un solo titolare del trattamento e non da piu' strutture sanitarie in qualita' di autonomi titolari, come avviene proprio per il Fse.

Cio' stante, molte delle misure individuate a tutela della protezione dei dati in occasione dell'esame dei testi normativi relativi all'istituzione del Fse si ritiene debbano trovare applicazione anche con riferimento ai trattamenti effettuati mediante il dossier sanitario.

1. Linee guida in materia di dossier sanitario

Nel corso degli ultimi anni, il Garante e' intervenuto piu' volte, d'Ufficio o a seguito di segnalazioni, con i richiamati provvedimenti prescrittivi relativi ai trattamenti di dati personali effettuati da strutture sanitarie attraverso lo strumento del dossier sanitario.

A fronte dell'incremento dell'uso di tali strumenti da parte delle strutture sanitarie e della complessita' della materia in rapporto alla disciplina sul trattamento dei dati personali, con l'adozione delle «Linee guida in materia di dossier sanitario» («Allegato A»), che formano parte integrante della presente deliberazione, il Garante intende fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte e conformare i trattamenti ai principi di legittimita' stabiliti dal Codice, nel rispetto di elevati standard di sicurezza. A tal scopo, l'Autorita' ritiene opportuno riportare nell'«Allegato C» alla presente deliberazione le definizioni dei principali vocaboli utilizzati nelle Linee guida, facendo riferimento sia a definizioni previste dalle disposizioni vigenti in materia sia ai termini generalmente utilizzati nell'ambito della sanita' digitale con riferimento ai quali non e' ancora intervenuta una definizione normativa.

2. Comunicazione di violazione dei dati personali trattati attraverso il dossier sanitario

Le peculiari caratteristiche del trattamento dei dati sopra descritto, la particolare delicatezza delle informazioni trattate, nonche' l'esigenza di garantire l'esattezza, l'integrita' e la disponibilita' dei dati, unitamente agli specifici rischi di accesso non autorizzato e di trattamento non consentito illustrati nelle Linee guida allegate, fanno ritenere necessario assoggettare il loro trattamento, anche in coerenza con le previsioni normative in tema di Fse, all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware...) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione. La mancata comunicazione al Garante configura un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter del Codice.

A questo fine, entro quarantotto ore dalla conoscenza del fatto, i titolari del trattamento dei dati sono tenuti a comunicare all'Autorita' tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'«Allegato B» alla presente deliberazione e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.dossier@pec.gpdp.it.

3. Diritto alla visione degli accessi al dossier sanitario

In considerazione di quanto emerso nel corso delle attivita'

istruttorie svolte dall'Ufficio in merito al trattamento di dati personali effettuato mediante il dossier sanitario e, in particolare, dei lamentati accessi al dossier da parte di personale amministrativo o sanitario che non era stato mai coinvolto nel processo di cura dell'interessato, l'Autorita' ritiene necessario, anche in coerenza con le previsioni normative in tema di Fse, riconoscere all'interessato il diritto alla visione degli accessi al proprio dossier sanitario. Cio' stante, l'interessato puo' avanzare una formale richiesta al titolare del trattamento o a un suo delegato, al fine di conoscere gli accessi eseguiti sul proprio dossier con l'indicazione della struttura/reparto che ha effettuato l'accesso, nonche' della data e dell'ora dello stesso.

Il titolare del trattamento o un suo delegato devono fornire riscontro alla suddetta richiesta dell'interessato entro 15 giorni dal suo ricevimento. Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessita', ovvero ricorre altro giustificato motivo, il titolare o un suo delegato ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro e' di 30 giorni dal ricevimento della richiesta medesima.

Tutto cio' premesso il garante

1. adotta, ai sensi dell'art. 154, comma 1, lettera h), del Codice, le «Linee guida in materia di dossier sanitario» e le «Definizioni» contenute rispettivamente nell'«Allegato A» e nell'«Allegato C», che formano parte integrante della presente deliberazione, al fine di informare i titolari di trattamenti e gli interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza, e sui presupposti di legittimita' dei trattamenti dei dati personali effettuati attraverso il dossier sanitario;

2. prescrive, ai sensi dell'art. 154, comma 1, lettera c), del Codice, che i titolari di trattamenti comunichino al Garante, entro quarantotto ore dalla conoscenza del fatto, le violazioni dei dati personali trattati attraverso il dossier sanitario secondo le modalita' di cui al paragrafo 2 del presente provvedimento e lo schema riportato nell'«Allegato B» che forma parte integrante della presente deliberazione;

3. prescrive, ai sensi dell'art. 154, comma 1, lettera c), del Codice, che i titolari di trattamenti forniscano all'interessato, che abbia manifestato il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, un riscontro alla richiesta avanzata dallo stesso o da un suo delegato volta a conoscere gli accessi eseguiti sul proprio dossier con l'indicazione della struttura/reparto che ha effettuato l'accesso, della data e dell'ora dello stesso, secondo le modalita' di cui al paragrafo 3 del presente provvedimento;

4. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia - Ufficio pubblicazione leggi e decreti - per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

La presente deliberazione, considerata la sua valenza generale, e' inviata alle regioni e province autonome affinche' provvedano a divulgarla presso le strutture sanitarie competenti.

Roma, 4 giugno 2015

Il Presidente
Soro

Il relatore
Califano

Il segretario generale

Busia

Allegato A

Parte di provvedimento in formato grafico

Allegato B

Parte di provvedimento in formato grafico

Allegato C

Parte di provvedimento in formato grafico