VEDI ANCHE Newsletter del 26 novembre 2015

[doc. web n. 4449114]

Dossier sanitario: prescrizioni per il sistema informativo delle prestazioni sanitarie erogate da un'Azienda sanitaria - 22 ottobre 2015

Registro dei provvedimenti
n. 550 del 22 ottobre 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza 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 Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), di seguito "Codice";

VISTA la segnalazione ricevuta concernente il sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dall'Azienda USL 11 di Empoli;

VISTE la richieste di informazioni in atti;

VISTI gli atti dell'accertamento ispettivo effettuato dall'Ufficio presso l'Azienda USL 11 di Empoli il 30 marzo 2015;

VISTA la documentazione inviata dall'Azienda USL 11 di Empoli a seguito del suddetto accertamento ispettivo e della richiesta di informazioni in atti;

VISTO le "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario" adottate dal Garante con Provvedimento del 16 luglio 2009 (G.U. n. 178 del 3 agosto 2009, consultabili sul sito www.gpdp.it, doc. web n. 1634116);

VISTO l'articolo 12 (Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario) del decreto legge 18 ottobre 2012 n. 179, convertito, con modificazioni, dall'art. 1, comma 1, legge 17 dicembre 2012, n. 221;

VISTE le "Linee guida in materia di Dossier sanitario" adottate dal Garante con Provvedimento del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015, doc. web n. 4084632);

VISTI gli atti d'Ufficio;

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

RELATORE la prof.ssa Licia Califano;

PREMESSO

E' pervenuta a questa Autorità una segnalazione nella quale si lamenta una presunta violazione della disciplina in materia di protezione dei dati personali relativamente alle modalità di funzionamento del sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dall'Azienda USL 11 di Empoli. Più precisamente, secondo quanto segnalato gli applicativi in uso presso i diversi reparti dell'Azienda sarebbero stati configurati in modo tale da consentire a ogni medico di accedere non solo ai dati personali dei propri pazienti, ma anche a quelli di qualsiasi altra persona che sia stata in cura presso la struttura sanitaria. L'accesso del personale sanitario autorizzato sarebbe, pertanto, indipendente dalla circostanza che le informazioni che questi possono conoscere siano riferite a soggetti dagli stessi assistiti.

Il segnalante rappresenta, inoltre, di non aver prestato alcun consenso informato in relazione al suddetto trattamento di dati personali.

A seguito di tale segnalazione, l'Ufficio ha richiesto informazioni alla predetta Azienda con particolare riferimento alla possibilità di ricondurre il suddetto sistema informativo al concetto di dossier indicato nel provvedimento del Garante del 16 luglio 2009 concernente "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario" e, conseguentemente, al rispetto, nella sua implementazione, delle garanzie individuate nelle Linee guida del 2009 citate.

Nella risposta alla richiesta di informazioni, l'Azienda ha affermato di avvalersi "di un sistema clinico informativo ospedaliero fortemente integrato ("Galileo")" e di essere in procinto di realizzare un "progetto aziendale di adeguamento" per "ottemperare alle norme" e "agli

indirizzi applicativi vigenti in materia di trattamento dei dati personali.

Alla luce del suddetto riscontro, l'Ufficio procedeva ad effettuare il 30 marzo 2015 un accertamento ispettivo presso l'Azienda USL 11 di Empoli, volto a verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, con particolare riferimento a quanto indicato nelle richiamate Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario.

Durante i suddetti accertamenti ispettivi è stato verificato che il sistema informativo in uso presso la suddetta Azienda -denominato Galileo- è finalizzato a gestire il percorso di cura dei pazienti che si rivolgono alla stessa e può essere inquadrato nella definizione di dossier sanitario di cui alle menzionate Linee guida del Garante.

Secondo quanto dichiarato in atti dai rappresentati dell'Azienda, nel sistema Galileo sono presenti circa 354.000 dossier sanitari relativi a soggetti che hanno effettuato almeno un accesso all'Azienda USL 11 di Empoli (stima relativa al mese di aprile 2015).

Tale sistema informativo è stato scelto in via autonoma dalla predetta Azienda come strumento di gestione dei dati sanitari dei pazienti per finalità di cura degli stessi e per le finalità amministrative correlate.

Il sistema, utilizzato nella totalità dei reparti (ad esclusione del Pronto Soccorso (DEA)) ed in quasi tutte le strutture ambulatoriali, è implementato anche con i dati e i documenti provenienti dalla radiologia, dalla diagnostica di laboratorio, da alcuni tracciati elettrocardiografici, dai verbali e dalle schede infermieristiche del DEA, nonché dagli esami di laboratorio e strumentali effettuati in emergenza. Tale sistema viene implementato anche con le informazioni relative alle prestazioni erogate in forma intramuraria.

In sede di accertamento ispettivo è emerso che gli utenti dell'Azienda USL 11 di Empoli abilitati ad accedere al sistema Galileo- mediante specifiche credenziali di autenticazione- sono circa 1.400 cui sono stati attribuiti, diversi profili di accesso in relazione ai ruoli e alle funzioni agli stessi attribuite.

Secondo quanto rilevato in sede ispettiva, il personale sanitario (medico, infermieristico e farmacisti operanti presso l'Azienda) accede al sistema Galileo esclusivamente per finalità di cura. In prima battuta il suddetto personale visualizza -tramite Galileo- il dossier sanitario di tutti i pazienti assistiti dalla struttura di assegnazione di chi effettua l'accesso. E' stato, altresì, verificato che per i reparti di degenza il sistema Galileo fornisce, prima facie, una visualizzazione del dossier di ogni paziente ricoverato o dimesso dal reparto a cui appartiene il sanitario che effettua l'accesso nei 60 giorni precedenti. Tuttavia, attraverso la funzione denominata "reparto corrente" il personale sanitario ha la possibilità di accedere anche al dossier di tutti i soggetti ricoverati o dimessi da meno di 6 mesi da tutti i reparti dell'Azienda o che hanno ricevuto una prestazione ambulatoriale nei 3 mesi precedenti alla data dell'accesso. Secondo quanto dichiarato in atti dai rappresentati dell'Azienda, tale ultima funzionalità sarebbe stata realizzata anche per consentire l'accesso al sistema da parte del personale coinvolto nella "Guardia Inter divisionale" (continuità assistenziale), nei consulti e nei servizi resi nei giorni festivi e prefestivi.

Secondo quanto dichiarato dall'Azienda nella documentazione in atti, tra i 1400 utenti abilitati, il personale sanitario che può accedere al dossier relativo a soggetti non più ricoverati o che abbiano in passato usufruito di una prestazione ambulatoriale supera i 900 utenti. Tra questi circa 70 utenti (personale sanitario) sono anche abilitati ad accedere al dossier al di fuori della rete aziendale, attraverso l'utilizzo di un client di connettività e un duplice processo di identificazione, autenticazione e autorizzazione.

Secondo quanto emerso in sede ispettiva e dalla documentazione inviata successivamente dall'Azienda, al sistema Galileo può accedere – tramite l'attribuzione di uno specifico profilo- anche la direzione sanitaria. Tale accesso è consentito per finalità di programmazione e valutazione dei processi clinici assistenziali, per la fase istruttoria correlata alle azioni di risarcimento o legali in cui è coinvolta l'Azienda, nonché per la sorveglianza delle infezioni correlate all'assistenza. Gli utenti della direzione sanitaria abilitati con tale profilo (circa 6) possono accedere a Galileo senza alcuna restrizione in ordine alle funzioni di ricerca o all'arco temporale in cui effettuare la stessa.

In sede ispettiva è stato constato, inoltre, che anche il personale appartenente all'Ufficio relazioni con il pubblico (URP) può avere accesso al sistema Galileo, al fine di fornire notizie sui ricoveri a terzi nel rispetto della manifestazione di volontà espressa al riguardo dal paziente, per la gestione dei reclami, segnalazioni o esposti dei pazienti, nonché per la gestione delle pratiche di richiesta della cartella clinica. Al riguardo, è stato constatato che il sistema è stato configurato in modo tale da consentire agli operatori con profilo URP -attraverso la funzione "ricerca"- di accedere al dossier (senza dati di dettaglio) relativo sia ai soggetti già dimessi (senza limite temporale) che a quelli ricoverati al momento dell'accesso al sistema (nei confronti dei quali, quindi, non è ancora possibile richiedere la cartella clinica). Tale ricerca è possibile anche inserendo solo porzioni di cognome.

Durante il predetto accertamento ispettivo è stato constatato che al sistema Galileo è possibile accedere (attraverso l'attribuzione di uno specifico profilo) anche da parte del personale addetto all'accettazione, dimissione e trasferimento dei pazienti ("Sportello ADT"). Secondo quanto dichiarato dai rappresentanti dell'Azienda in sede ispettiva e da quanto riportato nella documentazione successivamente inviata, tale accesso sarebbe finalizzato all'acquisizione dei dati necessari per assolvere al debito informativo verso la Regione Toscana e il Ministero della Salute (flusso schede di dimissione ospedaliera -SDO), per la gestione degli addebiti e rimborsi degli oneri relativi ai ricoveri, per il controllo dei corretti adempimenti di legge relativi alla tenuta delle cartelle cliniche. Tale accesso è consentito senza alcuna restrizione in ordine alle funzioni di ricerca o all'arco temporale in cui effettuare la stessa.

E' stato, poi, constatato che al sistema Galileo è possibile accedere anche con il profilo di direzione medica di presidio ospedaliero. Attraverso tale profilo è possibile accedere ai dossier sanitari presenti sul sistema Galileo visualizzando tutte le informazioni presenti negli stessi senza alcuna restrizione in ordine alle funzioni di ricerca, anche da un punto di vista temporale. Secondo quanto dichiarato dai rappresentanti dell'Azienda in sede ispettiva e quanto riportato nella documentazione in atti, tale accesso sarebbe finalizzato al rilascio delle copie autentiche della documentazione sanitaria ospedaliera e alla verifica circa la correttezza della compilazione delle cartelle cliniche.

In sede ispettiva è, inoltre, emerso che l'accesso al sistema Galileo è consentito anche ai soggetti operanti presso la portineria dell'Azienda. In tal caso, è possibile visualizzare solo i dati essenziali a comunicare ai terzi legittimati l'ubicazione del paziente presso la struttura, laddove l'interessato abbia manifestato un consenso al riguardo.

Secondo quanto dichiarato negli atti dell'accertamento ispettivo per ogni accesso al sistema Galileo sono tracciate le operazioni di inserimento e modifica dei dati. Non sono invece tracciate le operazioni di visualizzazione e di stampa che, tuttavia, sono in fase di implementazione. Tale processo di implementazione avrà ad oggetto anche sistemi di alert automatizzati per il rilevamento di eventuali anomalie negli accessi (ad es., relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

In sede di accertamento ispettivo è emerso che il sistema Galileo è stato popolato a far data dal 2010 e che in esso è confluita tutta la documentazione clinica presente in Azienda riferibile ad eventi sanitari precedenti a tale data.

Con riferimento al trattamento di dati personali effettuato tramite il dossier sanitario i rappresentanti dell'Azienda hanno evidenziato in sede ispettiva che ai pazienti viene fornita una specifica informativa al riguardo solo dal mese di gennaio 2015 e che il consenso al dossier sanitario è richiesto a decorrere dal mese di febbraio 2015. Secondo quanto dichiarato, il consenso è acquisito oralmente da parte del medico e documentato su Galileo attraverso l'inserimento di un flag in un apposito riquadro denominato "consenso". In tale riquadro sarebbe annotata anche la manifestazione del consenso per il trattamento mediante il dossier dei dati sanitari raccolti dall'Azienda in data antecedente alla richiesta del consenso (c.d. "dati pregressi"); in caso di ricovero, stampa di tale manifestazione di volontà è inserita nella cartella clinica.

Come indicato nel verbale del richiamato accertamento ispettivo, prima delle date sopra richiamate l'Azienda USL 11 di Empoli non forniva l'informativa agli interessati e non acquisiva il consenso degli stessi per il trattamento dei dati personali effettuato tramite il dossier sanitario aziendale.

Con specifico riferimento alle modalità di revoca del consenso e di oscuramento delle informazioni consultabili attraverso il dossier, i rappresentanti dell'Azienda hanno specificato che le stesse sono espressamente indicate nell'informativa rilasciata ai pazienti e che tali diritti sono esercitabili attraverso la compilazione di appositi moduli acquisiti in atti. Al momento dell'accertamento ispettivo, in caso di richiesta di oscuramento e di revoca del consenso da parte dell'interessato, l'Azienda provvedeva a comunicare al fornitore del sistema Galileo tali volontà; il fornitore poi procedeva ad effettuare i necessari interventi sul sistema per soddisfare le istanze dell'interessato. Secondo quanto dichiarato in atti, a far data dal mese di giugno 2015, attraverso l'installazione della nuova versione del sistema informativo, le operazioni di revoca del consenso e di oscuramento sono effettuate da parte di personale interno all'Azienda attraverso una apposita funzione presente su Galileo.

OSSERVA

1. Premessa.

La tematica del trattamento di dati personali effettuato tramite il dossier sanitario utilizzato presso le strutture sanitarie è stata affrontata dall'Autorità sin dal 2009 con il citato provvedimento del 16 luglio adottato a seguito di una consultazione pubblica.

Secondo la definizione resa nelle citate Linee guida del 2009, poi ribadita nelle successive Linee guida del 4 giugno 2015, il dossier sanitario è lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale, azienda sanitaria, casa di cura) al cui interno operino più 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.

Nel corso degli ultimi anni, il Garante è intervenuto più 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. Tali provvedimenti, adottati a seguito di specifiche attività ispettive svolte presso strutture sanitarie pubbliche, hanno evidenziato forti criticità nell'adozione delle prescrizioni contenute nel Codice relative ai trattamenti di dati idonei a rivelare lo stato di salute effettuati per finalità di cura.

Alla luce dell'esperienza acquisita a seguito delle richiamate attività ispettive e dei provvedimenti prescrittivi conseguentemente adottati, nonché in considerazione dell'incremento dell'uso di tali strumenti da parte delle strutture sanitarie l'Autorità ha recentemente adottato un nuovo provvedimento recante "Linee guida in materia di dossier sanitario" (Provvedimento citato del 4 giugno 2015 - di seguito Linee guida del 2015). Attraverso tale provvedimento il Garante, nel ribadire quanto già indicato nelle Linee guida del 2009, ha inteso illustrare più compiutamente-anche alla luce dell'esperienza maturata- gli adempimenti in materia di protezione dei dati personali che i titolari che effettuano trattamenti di dati personali mediante il dossier sanitario devono porre in essere per conformare gli stessi ai principi di legittimità stabiliti dal Codice, nel rispetto di elevati standard di sicurezza.

Nelle suddette Linee guida l'Autorità ha da un lato ricordato gli adempimenti in materia di protezione dei dati personali trattati in ambito sanitario già previsti dal Codice e nelle Linee guida del 2009, fornendo indicazione sulle modalità attuative degli stessi, e dall'altro prescritto che i titolari del trattamento comunichino al Garante, entro quarantotto ore dalla conoscenza del fatto, le violazioni dei dati personali trattati attraverso il dossier sanitario, nonché 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.

2. Profili di criticità.

In base a quanto emerso nel corso del richiamato accertamento ispettivo e dall'esame della documentazione in atti, alcune delle specifiche garanzie previste dal Codice e richiamate nelle citate Linee guida del 2009 e del 2015 non sono state rispettate nel trattamento dei dati personali effettuati attraverso il dossier sanitario attualmente in uso presso l'Azienda USL 11 di Empoli.

L'Autorità prende atto che subito dopo il predetto accertamento ispettivo l'Azienda ha posto in essere azioni migliorative dello stato degli adempimenti in materia di protezione dei dati personali, in particolare, in ordine alle designazioni a responsabile esterno del trattamento e

alla scelta di specifiche misure di sicurezza.

Tali azioni, tuttavia, non superano tutte le criticità riscontrate in sede ispettiva e di esame documentale degli atti inviati all'Autorità successivamente agli accertamenti in loco. Il trattamento dei dati personali effettuato mediante il dossier sanitario aziendale presenta, infatti, ancora profili di criticità -nei termini specificati in dettaglio in seguito- con riferimento all'informativa al trattamento dei dati personali effettuato tramite il dossier sanitario aziendale, all'accesso al dossier sanitario da parte del personale sanitario che assiste l'interessato, nonché all'utilizzo di tale strumento da parte del personale afferente alle strutture amministrative interne all'Azienda.

2.1 Informativa e consenso.

Come specificato da questa Autorità nelle citate Linee guida del 2009 e confermato nelle nuove Linee guida del 2015, il trattamento dei dati personali effettuato mediante il dossier, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di autodeterminazione (artt. 75 e ss. del Codice).

Nelle Linee guida del 2015, l'Autorità ha, in particolare, esplicitato ulteriormente che il trattamento dei dati personali effettuato tramite il dossier costituisce un trattamento aggiuntivo rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso. In assenza del dossier sanitario, infatti, il professionista avrebbe accesso alle sole informazioni fornite in quel momento dal paziente e a quelle elaborate in relazione all'evento clinico per il quale lo stesso ha richiesto una prestazione sanitaria; attraverso l'uso del dossier sanitario, invece, il professionista pone in essere un ulteriore trattamento di dati sanitari mediante la consultazione delle informazioni elaborate nell'ambito dell'intera struttura sanitaria e non solo del suo reparto e, quindi, da professionisti diversi, in occasione di altri eventi clinici occorsi in passato all'interessato che siano riferibili anche a patologie differenti rispetto all'evento clinico in relazione al quale l'interessato riceve la prestazione sanitaria (cfr. punto 2 delle citate Linee guida del 2015 e punto 3 delle Linee guida del 2009). In quanto tale, il trattamento dei dati personali effettuato mediante il dossier sanitario necessita di una specifica informativa che contenga tutti gli elementi previsti dall'art. 13 del Codice.

L'informativa deve indicare, tra l'altro, le finalità che la struttura sanitaria, in qualità di titolare, intende perseguire attraverso il trattamento dei dati personali effettuato mediante il dossier sanitario (art. 13, comma 1, lett. a) del Codice).

In tale ambito l'Autorità ha più volte ricordato che il titolare del trattamento deve evidenziare nell'informativa l'intenzione di costituire un insieme di informazioni personali riguardanti l'interessato il più possibile completo che documenti parte della storia sanitaria dello stesso, al fine di migliorare il suo processo di cura attraverso un accesso integrato di tali informazioni da parte del personale sanitario coinvolto.

Nell'informativa è necessario, inoltre, che sia specificata l'eventualità che il dossier sanitario sia consultabile anche da parte dei professionisti che agiscono in libera professione intramuraria -detta anche intramoenia- ovvero nell'erogazione di prestazioni al di fuori del normale orario di lavoro utilizzando le strutture ambulatoriali e diagnostiche della struttura sanitaria a fronte del pagamento da parte del paziente di una tariffa; analoga indicazione deve essere fornita anche qualora la consultazione sia ritenuta indispensabile, nel rispetto dell'Autorizzazione generale del Garante, per la salvaguardia della salute di un terzo o della collettività (cfr. punto 2 delle citate Linee guida del 2015).

Nell'indicare le finalità del trattamento è necessario che il titolare evidenzi l'eventualità che il dossier sia utilizzato anche per finalità amministrative correlate alla cura dell'interessato.

Tra gli elementi che devono essere indicati nell'informativa deve essere ricondotta anche l'indicazione dei diritti di cui agli artt. 7 e ss. del Codice e delle modalità attraverso le quali esercitare gli stessi. Tra tali diritti si evidenzia, in particolare, quello di ottenere la conferma circa l'esistenza o meno dei dati che lo riguardano, la loro comunicazione in forma intelligibile, l'indicazione della loro origine, delle finalità e modalità del trattamento (art. 7, comma 1 e 2, lett. a) e b), del Codice).

Essendo il dossier sanitario un trattamento di dati personali effettuato con modalità elettroniche atte a consentire una integrazione massiva di dati e documenti contenenti informazioni idonee a rivelare lo stato di salute, assume particolare rilievo il diritto riconosciuto all'interessato di poter ottenere l'indicazione della logica applicata a tale trattamento (art. 7, comma 2, lett. c), del Codice), ovvero l'indicazione dei criteri utilizzati nell'elaborazione elettronica dei dati.

Si evidenzia, inoltre, che il Codice riconosce all'interessato il diritto di ottenere l'indicazione del titolare del trattamento, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati (art. 7, comma 2, lett. e), del Codice).

Come meglio esplicitato dal Garante nelle Linee guida del 2015, nell'informativa devono essere indicate anche le modalità attraverso le quali l'interessato può chiedere di revocare il consenso all'implementazione del dossier sanitario e di oscurare alcuni eventi clinici presenti nello stesso (cfr. punti 2 e 5 delle Linee guida del 2015 e punto 8 delle Linee guida del 2009). Secondo quanto indicato nelle citate Linee guida del 2015 nell'informativa devono, poi, essere illustrate anche le modalità attraverso le quali l'interessato può esercitare il diritto alla visione degli accessi che sono stati effettuati al dossier sanitario (cfr. punto 5 delle Linee guida del 2015).

Ulteriore elemento che deve essere indicato nell'informativa è relativo alle designazioni a responsabile del trattamento che sono state effettuate dall'Azienda sanitaria. Qualora il titolare abbia designato più responsabili, infatti, l'informativa deve contenere l'indicazione di almeno uno di essi, nonché del sito della rete di comunicazione o di altra modalità attraverso la quale è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, deve essere indicato tale responsabile.

Essendo il trattamento dei dati personali effettuato tramite il dossier un trattamento facoltativo, all'interessato deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale

strumento, ed informandolo altresì che tale scelta non incide sulle cure mediche richieste (cfr. punti 2 e 3 delle citate Linee guida del 2015). Ciò significa che qualora l'interessato non manifesti il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (ad es., raccolta dell'anamnesi e delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista. Analogamente, in tale circostanza il personale sanitario di reparto/ambulatorio avrà accesso solo alle informazioni relative all'episodio per il quale l'interessato si è rivolto presso quella struttura e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio (c.d. accesso agli applicativi verticali dipartimentali) (cfr. punto 3 delle citate Linee guida del 2015).

Secondo quanto dichiarato in sede di accertamento ispettivo, l'Azienda USL 11 di Empoli -in qualità di titolare del trattamento- ha iniziato a raccogliere il consenso informato degli interessati in merito al trattamento dei dati personali effettuato mediante il dossier sanitario solo dal mese di febbraio 2015, sebbene tale strumento fosse in uso presso la stessa già dal 2010. Secondo quanto dichiarato in atti, l'Azienda ha trattato, quindi, i dati personali degli interessati mediante il dossier sanitario dal 2010 al febbraio 2015 senza aver acquisito il consenso informato degli stessi.

Dall'esame del modello di informativa acquisito in sede ispettiva e utilizzato dall'Azienda dal mese di febbraio 2015 emergono, inoltre, alcune criticità riconducibili alla circostanza che all'interessato non sono stati forniti alcuni elementi previsti dall'art. 13 del Codice.

In particolare, nel modello di informativa in atti non sono state indicate compiutamente le finalità perseguite dall'Azienda nel trattamento dei dati personali effettuato mediante il dossier sanitario. Nel suddetto modello, infatti, l'Azienda ha dichiarato di perseguire esclusivamente finalità di cura dell'interessato e non anche finalità amministrative correlate alla cura, la cui realizzazione è stata rilevata in sede ispettiva attraverso l'esame delle funzionalità attribuite ai già indicati profili di abilitazione di direzione sanitaria, URP, Sportello ADT, direzione medica ospedaliera e portineria.

Si evidenzia, inoltre, che nell'illustrazione all'interno del modello di informativa in atti delle finalità di cura perseguite attraverso il trattamento dei dati personali effettuato tramite il dossier non è specificato che tale strumento è utilizzato anche nell'ambito delle prestazioni sanitarie erogate in forma intramuraria.

Ulteriore elemento di cui risulta privo il modello di informativa in atti è relativo alla mancata indicazione all'interessato dei diritti riconosciuti allo stesso dall'art. 7 del Codice.

Nel suddetto modello sono poi fornite indicazioni in merito alla possibilità per l'interessato di revocare il proprio consenso e di oscurare alcuni eventi sanitari consultabili mediante il dossier senza, tuttavia, indicare le modalità attraverso le quali esercitare tali prerogative. Sebbene tale indicazione non sia riconducibile agli elementi essenziali dell'informativa previsti dal richiamato art. 13 del Codice, l'Autorità, nelle citate Linee guida del 2009 e del 2015, ha auspicato che l'interessato, attraverso l'informativa, sia messo a conoscenza delle modalità attraverso le quali esercitare tali facoltà (cfr. punto 8 delle Linee guida del 2009 e punti 2 e 5 delle Linee guida del 2015).

Il modello di informativa acquisito in atti, inoltre, non riporta l'indicazione dei responsabili del trattamento o delle modalità attraverso le quali è possibile conoscere l'elenco delle suddette designazioni effettuate dal titolare (art. 7, comma 1, lett. f) del Codice).

Pertanto, con riferimento al trattamento di dati personali effettuato dall'Azienda USL 11 di Empoli mediante il suddetto dossier, si rileva che, al momento degli accertamenti ispettivi, il modello di informativa fornito all'Ufficio presentava profili di criticità, nei termini sopra descritti. Ciò premesso, l'Autorità, al fine di rendere conforme il trattamento dei dati effettuato dall'Azienda USL 11 di Empoli, in qualità di titolare del trattamento, attraverso lo strumento del dossier, ritiene necessario che i modelli di informativa in uso presso l'Azienda siano integrati con l'indicazione:

a) di tutte le finalità perseguite attraverso il trattamento dei dati personali effettuato mediante il dossier sanitario, avendo cura di precisare che le finalità di prevenzione, diagnosi e cura sono perseguite altresì attraverso l'erogazione di prestazioni sanitarie in forma intramuraria e che attraverso il dossier sanitario l'Azienda persegue anche finalità amministrative correlate alla cura mediante il trattamento delle sole informazioni a ciò indispensabili;

b) dei diritti di cui all'art. 7 del Codice;

c) degli estremi identificativi di un responsabile del trattamento, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili;

d) delle modalità attraverso le quali è possibile richiedere la revoca del consenso al trattamento dei dati effettuato mediante il dossier sanitario e l'oscuramento delle informazioni relative a uno o più eventi clinici trattate mediante il dossier;

e) del diritto alla visione degli accessi al dossier individuato dal Garante con il citato Provvedimento del 4 giugno 2015 (Linee guida in materia di dossier sanitario).

Tali integrazioni all'informativa dovranno essere effettuate entro il 31 marzo 2016 (artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice).

L'Autorità, in relazione agli aspetti sopra rappresentati, ritiene, inoltre, necessario riservarsi di verificare, con autonomo procedimento, la sussistenza dei presupposti per contestare all'Azienda USL 11 di Empoli le violazioni delle disposizioni di cui agli artt. 13 e 23, del Codice e la conseguente applicazione delle sanzioni di cui agli artt. 161 e 162, comma 2-bis del Codice con riferimento al trattamento dei dati personali effettuato attraverso il dossier dal 2010 al 2015, nonché con riferimento all'inidoneità dell'informativa fornita dall'Azienda a partire dal 2015.

2.2 Accesso al dossier sanitario da parte del medico che ha in cura l'interessato.

Nelle citate Linee guida del 2015 il Garante, con riferimento all'accesso ai dati contenuti nel dossier sanitario, ha ribadito quanto già previsto nelle Linee guida del 2009 in ordine alla circostanza che l'accesso a tale strumento deve essere limitato al personale sanitario che interviene nel tempo nel processo di cura del paziente (cfr. punto 6 delle Linee guida del 2015 e punto 5 delle Linee guida del 2009). Ciò significa che deve essere consentito l'accesso a tutto il personale che a vario titolo interviene nel processo di cura, come ad esempio quello operante nel reparto in cui è ricoverato il paziente, o che è stato coinvolto nella richiesta di una consulenza o nell'ambito delle procedure di un trapianto.

Al fine di consentire che abbia accesso al dossier solo il personale sanitario coinvolto -a vario titolo e nel tempo- nel processo di cura del paziente, devono essere adottate modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria. Il titolare del trattamento deve, pertanto, effettuare un monitoraggio delle ipotesi in cui il relativo personale sanitario può avere necessità di consultare il dossier sanitario, per finalità di cura dell'interessato e, in base a tale ricognizione, individuare i diversi profili di autorizzazione all'accesso.

L'accesso al dossier deve essere limitato, poi, al tempo in cui si articola il processo di cura, ferma restando la possibilità di accedere nuovamente al dossier qualora ciò si renda necessario in merito al tipo di trattamento medico da prestare all'interessato.

Alla data degli accertamenti ispettivi l'Azienda USL 11 di Empoli non aveva messo in atto specifiche procedure che consentissero al solo personale sanitario coinvolto nel processo di cura del paziente di accedere al relativo dossier per il tempo strettamente necessario alla cura. Dalla documentazione in atti risulta, infatti, che il personale sanitario che può accedere al dossier relativo sia ai pazienti attualmente in cura che a quelli non più ricoverati o che abbiano in passato usufruito di una prestazione ambulatoriale supera i 900 utenti.

Pertanto, al fine di rendere conforme il trattamento dei dati effettuato dall'Azienda USL 11 di Empoli, in qualità di titolare del trattamento, attraverso il dossier, il Garante ritiene necessario prescrivere alla predetta Azienda di mettere in atto di specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del dossier) di accedere al relativo dossier per il tempo in cui si articola il percorso di cura.

Il titolare del trattamento deve, pertanto, adottare soluzioni idonee a consentire che il professionista sanitario acceda al dossier dei pazienti in quel momento in cura presso lo stesso (ad es., medico di reparto rispetto al dossier relativo ai pazienti ricoverati; medico che opera in ambulatorio rispetto al dossier dei soggetti a cui in quel giorno deve essere erogata la prestazione ambulatoriale), ferma restando la possibilità per tali soggetti di consultare altri dossier sanitari motivando l'accesso sulla base di una casistica predeterminata dallo stesso titolare ed effettuata in base all'osservazione dei casi per i quali i professionisti generalmente accedono al dossier (ad es., trapianti, richiesta di consulenza, guardia medica, richiesta di chiarimenti terapeutici da parte dell'interessato) ovvero anche in ipotesi diverse da quelle predeterminate dal titolare documentando per iscritto la motivazione di tale accesso.

Tali accorgimenti devono essere completati entro il 31 marzo 2016 (artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice).

2.3 Accesso al dossier sanitario da parte di personale che svolge funzioni amministrative correlate alla cura.

Nelle Linee guida del 2015 il Garante ha meglio evidenziato rispetto alle Linee guida del 2009 che qualora il titolare del trattamento intenda utilizzare lo strumento del dossier sanitario anche per svolgere delle funzioni amministrative strettamente connesse con il percorso di cura del paziente (ad es., prenotazione di esami clinici; richiesta di copia delle cartelle cliniche; indicazione a terzi legittimati della presenza in reparto di un degente; gestione dei posti letto), deve prevedere delle limitazioni alla "profondità di accesso" al dossier da parte del personale preposto a tali funzioni, consentendo allo stesso di accedere ai soli dati indispensabili per svolgere i compiti ad essi demandati (cfr. punto 6 delle Linee guida del 2015 e punto 4 delle Linee guida del 2009).

Il personale amministrativo operante all'interno della struttura sanitaria in cui viene utilizzato il dossier può, pertanto, in qualità di incaricato del trattamento, consultare solo i dossier sanitari che riguardino i soggetti coinvolti nelle attività amministrative svolte, visualizzando le sole informazioni indispensabili per assolvere alle funzioni amministrative cui è preposto (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche può consultare unicamente i dossier di soggetti che stanno richiedendo una prestazione sanitaria visualizzando i soli dati indispensabili per la prenotazione stessa). Il titolare deve valutare, infatti, in relazione ai diversi profili di abilitazione, a quali dossier sia indispensabile accedere e con riferimento a questi rendere possibile la consultazione dei soli dati indispensabili per lo svolgimento delle attività cui è preposto l'utente abilitato (artt. 11, comma 1, lett. d) e 22, comma 5, del Codice) (ad es. escludendo la visibilità dei dati riferibili alla diagnosi o alla lettura dei referti).

Devono essere, pertanto, preferite soluzioni che consentano un'organizzazione modulare del dossier, 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 amministrativo per il quale è stata consentita l'accessibilità al dossier.

Il titolare del trattamento, inoltre, deve adottare soluzioni tali da garantire che l'accesso al dossier da parte del personale che svolge funzioni amministrative correlate alla cura sia limitato al periodo di tempo strettamente necessario ad assolvere a tali funzioni.

Secondo quanto dichiarato in atti, l'Azienda USL 11 di Empoli utilizza il dossier sanitario aziendale anche per perseguire finalità amministrative correlate alla cura relative alla possibilità di fornire notizie sui ricoveri o sull'ubicazione del paziente nella struttura a terzi nel rispetto della manifestazione di volontà espressa al riguardo dal paziente, alla gestione dei reclami, segnalazioni o esposti dei pazienti, nonché alla trattazione delle pratiche di richiesta della cartella clinica ("profilo URP" - "profilo portineria").

Secondo quanto dichiarato in atti, solo con riferimento al richiamato "profilo portineria" l'Azienda sanitaria, alla data dell'accertamento ispettivo, aveva già messo in atto specifici accorgimenti che consentivano al personale cui è attribuito tale profilo di visualizzare attraverso la consultazione del dossier le sole informazioni indispensabili per assolvere alle funzioni loro preposte. Per nessuno dei profili attribuiti al

personale che svolge funzioni amministrative sono state adottate soluzioni tali da consentire che lo stesso possa accedere al dossier dei soli soggetti interessati dall'attività amministrativa posta in essere (es. accesso al dossier dei soli soggetti che hanno richiesto copia di un cartella clinica) e per il tempo a ciò strettamente necessario.

Dalla documentazione in atti, inoltre, emerge che l'Azienda USL 11 di Empoli utilizza il dossier sanitario aziendale anche per finalità di programmazione e valutazione dei processi clinici assistenziali, per la fase istruttoria correlata alle azioni di risarcimento o legali in cui è coinvolta l'Azienda, nonché per la sorveglianza delle infezioni correlate all'assistenza ("profilo direzione sanitaria"), per l'acquisizione dei dati necessari per assolvere al debito informativo verso la Regione Toscana e il Ministero della Salute (flusso schede di dimissione ospedaliera -SDO), per la gestione degli addebiti e rimborsi degli oneri relativi ai ricoveri, per il controllo dei corretti adempimenti di legge relativi alla tenuta delle cartelle cliniche ("profilo sportello ADT"), nonché per il rilascio delle copie autentiche della documentazione sanitaria ospedaliera e alla verifica circa la correttezza della compilazione della cartelle cliniche ("profilo direzione medica di presidio ospedaliero").

Secondo quanto dichiarato in atti attraverso tali profili è possibile accedere a tutti i dossier sanitari presenti sul sistema Galileo senza alcuna limitazione temporale (ad es. per le attività di predisposizione della difesa in giudizio dell'Azienda l'accesso non è limitato al dossier dei soli soggetti che hanno intentato causa all'Azienda ma a tutti i dossier visualizzabili attraverso Galileo).

Per tali profili di autorizzazione all'accesso non sono, inoltre, previsti limiti in merito alla profondità di accesso.

Al riguardo, si rappresenta che i soggetti preposti all'assolvimento di tali obblighi devono avere accesso ai soli dossier relativi ai soggetti interessati dall'attività amministrativa posta in essere e con riferimento a questi comunque alle sole informazioni indispensabili ad assolvere a tali obblighi. Inoltre, si rappresenta che, qualora non fossero previsti moduli distinti all'interno del dossier per l'esercizio delle suddette funzioni, l'utilizzo di tali strumenti, per l'assolvimento dei predetti debiti informativi, potrebbe portare al paradosso secondo cui, laddove l'interessato non abbia manifestato il proprio consenso al dossier sanitario o abbia esercitato l'oscuramento di alcuni dati o documenti, la struttura sanitaria non potrebbe assolvere al debito informativo previsto dalla legge (a titolo esemplificativo si richiama quanto previsto dal decreto del Ministro della sanità 27 ottobre 2000, n. 380, e successive modificazioni, concernente l'aggiornamento della disciplina del flusso informativo sui dimessi dagli istituti di ricovero pubblici e privati).

Come già evidenziato dal Garante nelle Linee guida del 2015, si precisa che eventuali richieste dell'Autorità giudiziaria con riferimento ai dati o ai documenti accessibili mediante il dossier devono essere soddisfatte nel rispetto dei limiti stabiliti dalla legge, ma non possono costituire una base legittimante la raccolta dei dati. Più precisamente, il titolare del trattamento potrà fornire, nei limiti di legge, all'Autorità giudiziaria le informazioni in suo possesso, non costituendo l'eventualità che in futuro si presentino tali istanze un'idonea fonte legittimante la raccolta di dati personali dell'interessato.

Pertanto, al fine di rendere conforme il trattamento dei dati effettuato dall'Azienda USL 11 di Empoli, in qualità di titolare del trattamento, attraverso il dossier, il Garante ritiene necessario prescrivere alla predetta Azienda di mettere in atto di specifici accorgimenti che consentano al personale amministrativo di accedere al dossier dei soli soggetti che sono coinvolti nell'attività amministrativa per la quale è necessario l'accesso e comunque con riferimento alle sole informazioni indispensabili per assolvere alle funzioni amministrative cui sono preposti. L'accesso deve essere limitato al tempo strettamente necessario per perseguire l'attività cui è preposto il soggetto che effettua l'accesso.

Tali accorgimenti devono essere completati entro il 31 marzo 2016 (artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice).

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive all'Azienda USL 11 di Empoli, quali misure necessarie, di:

a) integrare il modello di informativa previsto dall'art.13 del Codice in uso per i trattamenti di dati personali effettati mediante il dossier sanitario con quanto indicato nel paragrafo 2.1 del presente provvedimento ed, in particolare, con l'indicazione:

1. delle finalità perseguite attraverso il trattamento dei dati personali effettuato mediante il dossier sanitario, avendo cura di precisare che le finalità di prevenzione, diagnosi e cura sono perseguite anche attraverso l'erogazione di prestazioni sanitarie in forma intramuraria e che attraverso il dossier sanitario l'Azienda persegue anche finalità amministrative correlate alla cura mediante il trattamento delle sole informazioni a ciò indispensabili;

2. dei diritti di cui all'art. 7 del Codice;

3. degli estremi identificativi di un responsabile del trattamento, indicando il sito della rete di comunicazione o altra modalità attraverso la quale è conoscibile in modo agevole l'elenco aggiornato dei responsabili;

4. delle modalità attraverso le quali è possibile richiedere la revoca del consenso al trattamento dei dati effettuato mediante il dossier sanitario e l'oscuramento delle informazioni relative a uno o più eventi clinici trattate mediante il dossier;

5. del diritto alla visione degli accessi al dossier individuato dal Garante con il Provvedimento del 4 giugno 2015 (Linee guida in materia di dossier sanitario).

Tali integrazioni dell'informativa devono essere effettuate entro il 31 marzo 2016;

b) mettere in atto, secondo quanto indicato nel paragrafo 2.2, specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in quel momento in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del dossier) di accedere al relativo dossier sanitario per il tempo in cui si articola il percorso di cura. Il titolare del trattamento deve, inoltre, adottare specifici accorgimenti affinché il professionista sanitario acceda al dossier dei soli pazienti in quel momento in cura presso lo stesso, ferma restando la possibilità per tali soggetti di consultare altri dossier sanitari motivando l'accesso sulla base di una casistica predeterminata dallo stesso ovvero anche in ipotesi diverse da quelle predeterminate dal titolare documentando per iscritto la motivazione di tale accesso.

Tali misure devono essere effettuate entro il 31 marzo 2016;

c) mettere in atto, secondo quanto indicato nel paragrafo 2.3, specifici accorgimenti che consentano al personale amministrativo di accedere al dossier dei soli soggetti che sono coinvolti nell'attività amministrativa per la quale è necessario l'accesso e comunque con riferimento alle sole informazioni indispensabili per assolvere alle funzioni amministrative cui sono preposti. L'accesso deve essere, inoltre, limitato al tempo strettamente necessario per perseguire l'attività cui è preposto il soggetto abilitato.

Tali misure devono essere effettuate entro il 31 marzo 2016.

Ai sensi dell'art. 157 del Codice, richiede all'Azienda USL 11 di Empoli, di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto previsto nelle precedenti lettere a), b) e c) del presente provvedimento e di fornire comunque riscontro entro trenta giorni dalla ricezione dello stesso. Si ricorda che il mancato riscontro alla richiesta ex art. 157 è punito con la sanzione amministrativa di cui all'art. 164 del Codice.

Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'Autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 22 ottobre 2015

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia