Provvedimento del 4 agosto 2025 [10166336]

VEDI ANCHE Newsletter del 25 settembre 2025

[doc. web n. 10166336]

Provvedimento del 4 agosto 2025*
Il Tribunale di Firenze, con sentenza n. 1947/2026 del 9/04/2026, ha ridotto la sanzione irrogata dall'Autorità con il provvedimento n. 474 del 4 agosto 2025 a € 20.000,00

Registro dei provvedimenti
n. 474 del 4 agosto 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Angelo Fanizza, 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. 30 giugno 2003, n. 196 recante "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 (di seguito "Codice");

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

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n.9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, in www.gpdp.it, doc. web n.1098801;

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. L'attività ispettiva

In data XX e XX, è stato svolto un accertamento ispettivo presso l'Azienda Ospedaliero-Universitaria Careggi (di seguito l'"Azienda"), al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali nel trattamento dei dati effettuato attraverso il dossier sanitario con particolare riferimento a quanto indicato nelle Linee guida del Garante del 4 giugno 2015 (di seguito anche solo "Linee Guida")

Nel corso della predetta attività ispettiva è stato accertato che l'Azienda utilizza due applicativi denominati "XX" e "XX" relativi, rispettivamente, alla cartella ambulatoriale e a quelle di ricovero, attraverso i quali è possibile effettuare delle ricerche, anche storiche, sui pazienti e da cui è possibile accedere, sulla base dei profili di autorizzazione concessi, alle cartelle ambulatoriali e di ricovero presenti negli applicativi verticali utilizzati dalle unità operative aziendali. Negli applicativi verticali sono registrate tutte le prestazioni sanitarie erogate dalle strutture operative interne all'Azienda anche se rese in regime di intramoenia.

Secondo quanto indicato nel verbale delle operazioni compiute il XX, i citati applicativi, consentendo di effettuare ricerche sui documenti sanitari storici di un paziente, sono riconducibili al dossier sanitario secondo quanto indicato nelle predette Linee guida.

In merito agli adempimenti di cui alle Linee guida, l'Azienda ha precisato che, sebbene inizialmente fosse stata prevista un'informativa sul dossier, ancora oggi visibile sul sito aziendale, e fosse stata predisposta nel regolamento aziendale del XX una specifica sezione dedicata a tale strumento informativo, tale documentazione non è stata di seguito aggiornata sulla base delle novità introdotte dal Regolamento.

Nel corso delle predette operazioni è stato dichiarato inoltre che i pazienti attualmente registrati in tali applicativi sono XX, specificando che vi sono XX cartelle di degenza relative a XX pazienti e XX cartelle ambulatoriali relative a XX pazienti. Gli operatori attivi - che hanno effettuato almeno un accesso negli ultimi 3 mesi - attualmente abilitati ad accedere ai predetti applicativi sono XX. In totale, nel tempo, sono stati abilitati oltre XX operatori. Secondo quanto dichiarato in atti, alla data dell'accertamento ispettivo, non erano pervenute all'Azienda segnalazioni da parte degli interessati, in merito all'utilizzo delle funzioni relative al dossier sanitario accessibile attraverso gli applicativi "XX" e "XX".

Con specifico riferimento al consenso al trattamento dei dati effettuato attraverso il dossier sanitario aziendale, è stato dichiarato che all'epoca degli accertamenti ispettivi, non era fornita una specifica informativa e non era acquisito il consenso con riferimento a tali trattamenti, sebbene sul sito aziendale fosse presente la citata informativa sul trattamento dei dati non più aggiornata fino ai predetti accertamenti.

Sul punto, è stato precisato che, fino alla data delle verifiche ispettive, a prescindere da specifici progetti, al paziente veniva richiesto un solo consenso al trattamento dei dati personali per fini di cura che corrisponde a quello che era previsto dagli artt. 75 e ss. del Codice prima della revisione operata dal d.lgs n. 101/2018 a seguito della piena applicazione del Regolamento. Tale consenso era acquisito oralmente dall'operatore sanitario e tale operazione veniva registrata nei predetti applicativi mediante apposito flag.

In merito ai diritti esercitabili dall'interessato sui trattamenti effettuati attraverso il dossier, fermo restando che non era fornita alcuna informativa agli interessati, gli stessi non erano a conoscenza dell'esistenza di un trattamento che li riguardasse, è stato dichiarato che all'epoca degli accertamenti l'interessato poteva chiedere l'oscuramento solamente dell'intera cartella sanitaria. In tal caso, il medico aveva a disposizione una funzione denominata "gestione segreto professionale", accessibile in più modi, sia attraverso "XX" e "XX", che consentiva di oscurare attraverso il flag "oscura XX" tutta la cartella sanitaria. In caso di oscuramento, tutti i medici non abilitati alla unità operativa in cui si era verificato l'evento sanitario (ricovero o ambulatorio) non potevano accedere a quella oscurata che risultava, quindi, non visibile. Di tali facoltà il paziente non veniva specificamente informato.

Inoltre, non erano previsti oscuramenti parziali dei documenti di cui si compone la cartella di degenza a eccezione della relazione di degenza. Non vi erano casistiche di oscuramento automatico di dati, documenti e cartelle sanitarie neanche per i dati/prestazioni c.d. soggette a maggior tutela.

Nel corso del predetto accertamento è stato inoltre dichiarato che, in linea teorica, l'interessato poteva chiedere anche di avere visione degli accessi effettuati sulle cartelle sanitarie che lo riguardavano, sebbene allo stesso non fossero fornite informazioni puntuali in merito all'esercizio di tale diritto. Sulla base di quanto dichiarato in atti, negli ultimi anni è stata effettuata una sola richiesta (soddisfatta) di avere visione degli accessi effettuati sulla propria cartella sanitaria.

Relativamente alle modalità con cui sono attribuiti i profili di autorizzazione previsti per l'accesso al dossier da parte del personale sanitario è stato specificato che l'abilitazione era concessa, sulla base del profilo professionale, da utenti "amministratori" (1 o 2) designati dal direttore dell'unità operativa. Nelle unità operative, gli amministratori medici attribuivano i profili al personale medico e gli amministratori con il ruolo di coordinatore infermieristico quelli relativi agli infermieri.

Qualsiasi figura professionale poteva essere abilitata per area tematica, che comprende più unità operative, mentre per le sole unità operative alcuni profili non potevano essere abilitati (es. infermieri). Gli amministratori quando attribuivano un profilo di autorizzazione avevano delle funzioni previste di default; in ogni caso l'amministratore poteva decidere di ridurre le funzioni di ciascun profilo di abilitazione. Non vi erano indicazioni predeterminate fornite dall'Azienda sulle regole per l'attribuzione dei predetti profili.

Il soggetto abilitato poteva accedere con procedure di autenticazione informatica basate su sistemi di autenticazione a due fattori.

In relazione a quanto dichiarato, durante i predetti accertamenti ispettivi è stato accertato, mediante accesso con profilo "medico super user" all'applicativo "XX" dell'Azienda che:

> per i soli pazienti ricoverati, era possibile visualizzare la piantina dei letti dei degenti con riferimento ai quali il medico poteva accedere solo alle cartelle sanitarie -anche storiche- di quelli della sua unità operativa o di quelli afferenti ad unità operative a cui è abilitato;
>
> per i pazienti, anche non ricoverati, si poteva effettuare una ricerca per codice fiscale/STP (straniero temporaneamente presente) /numero cartella/codice nosologico/nome e cognome del paziente. Anche in questo caso il medico poteva accedere alle cartelle sanitarie dei pazienti afferenti alle unità operative a cui era abilitato. La ricerca con il parametro nome e cognome e codice fiscale restituiva l'elenco delle anagrafiche presenti nel gestionale: selezionando un elemento dell'elenco (paziente) si potevano consultare le relative cartelle sanitarie relative alle unità per le quali il medico era abilitato. Se la ricerca veniva effettuata attraverso il codice nosologico/numero cartella l'operatore accedeva direttamente alla cartella del paziente.

In entrambi i casi sopra descritti il medico, con riferimento ai pazienti ricoverati o che avevano una cartella ambulatoriale in una unità operativa a cui lo stesso era abilitato, poteva effettuare una ricerca sullo storico del paziente che gli restituiva l'elenco dei ricoveri e delle lettere al curante (a partire dal 1996 per l'unita di tossicologia) relative anche a unità operative diverse da quelle a cui lo stesso era abilitato. In tal caso, dopo aver dichiarato di aver acquisito il consenso verbale del paziente, il medico poteva accedere, per ciascuna cartella ambulatoriale o di ricovero sopra indicate, solo alla lettera al curante o alla relazione di degenza. Tali operazioni erano tracciate dal sistema.

L'Azienda ha inoltre precisato che il personale del reparto di emergenza e urgenza a eccezione dell'OBI (Osservazione Breve Intensiva) e dell'OB (Osservazione Breve) non accedeva agli applicativi "XX" e "XX" e, dunque, alle funzionalità del dossier.

In merito ai sistemi di tracciabilità degli accessi e delle operazioni effettuate attraverso il dossier sanitario aziendale è stato dichiarato che erano registrati, in appositi file di log, gli accessi agli applicativi degli operatori e le relative operazioni. In particolare, erano memorizzate le seguenti informazioni: identificativo operatore, data e ora, risorsa/pagina che indica l'operazione effettuata. Sono inoltre tracciati i login e logout degli operatori mediante registrazione delle seguenti informazioni: data e ora del login, modalità di

autenticazione. È stato inoltre dichiarato che al momento dell'accertamento ispettivo non vi erano sistemi di alert automatici o a campione.

Nel corso del predetto accertamento ispettivo l'Azienda ha dichiarato di voler avviare nell'immediato le azioni necessarie per conformare il dossier sanitario aziendale a quanto indicato nelle Linee guida del Garante del 2015 e ai principi e agli adempimenti previsti dal Regolamento.

Con le note del XX e XX, l'Azienda ha trasmesso documentazione utile a illustrare le "Azioni di miglioramento relative alle evidenze emerse nei verbali delle operazioni compiute dall'Ufficio del Garante per la protezione dei dati personali in data XX e XX presso l'Azienda Ospedaliero-Universitaria di Careggi".

Nella nota del XX, l'Azienda, nel dichiarare che l'"attività di trattamento assimilabili al Dossier Sanitario" sono state poste in essere "senza che gli specifici requisiti siano stati integralmente applicati" ha elencato le seguenti azioni correttive che ha avviato, attuato e messo in produzione:

blocco degli accessi e della visibilità delle cartelle attraverso il dossier sanitario, fino all'acquisizione del consenso informato del paziente;

aggiornamento delle informazioni rese ai sensi dell'art. 13 del Regolamento in relazione al trattamento effettuato tramite il dossier sanitario, sia fornite direttamente ai pazienti, sia mediante esposizione presso i punti di accettazione e sia sul sito istituzionale;

aggiornamento della modulistica e della procedura informatica necessaria all'acquisizione e alla revoca dei consensi relativi al trattamento effettuato attraverso il dossier mediante il personale impegnato nell'accettazione e identificazione del paziente. Il sistema informatico alla presenza del paziente, per ogni consenso richiesto (n. 3 consensi per: attivazione dossier, acquisizione eventi pregressi, inserimento dati "maggior tutela") genera un codice OTP che l'interessato deve prontamente comunicare per manifestare il proprio consenso. Ove l'interessato preferisca, gli operatori consentiranno, comunque, la manifestazione dei consensi su modulistica cartacea;

predisposizione di istruzioni specifiche per le persone autorizzate e i preposti al trattamento e aggiornamento del Regolamento interno limitatamente alla sezione dedicata al dossier sanitario con specifico riferimento al trattamento dei dati personali soggetti a maggior tutela dell'anonimato e alle modalità di acquisizione del consenso dei minori e del relativo aggiornamento al conseguimento della maggiore età;

aggiornamento delle procedure e della modulistica per l'esercizio dei diritti degli interessati (richiesta oscuramento, revoca dell'oscuramento, diritto alla visione degli accessi al dossier);

predisposizione policy per le attività di provisionig e deprovisioning degli accessi e contestuale verifica della c.d. profondità dell'accesso;

predisposizione della valutazione di impatto prevista dall'art. 35 del Regolamento.

Con la nota del XX, l'Azienda ha indicato le seguenti ulteriori azioni di miglioramento che sono state completate:

predisposizione di una procedura per l'analisi e la gestione delle violazioni di dati personali (data breach);

predisposizione di un corso di formazione specifico dedicato al dossier sanitario e di controlli a campione sugli accessi effettuati al dossier sanitario a partire da XX;

richiesta all'Estar (Ente di supporto regionale) di implementazione di misure di sicurezza adeguate con l'obiettivo di gestire, con soluzioni automatizzate, le attività di log management e audit log sugli applicativi utilizzati per i trattamenti effettuati attraverso il dossier sanitario;

Alla predetta data l'Azienda ha dichiarato di aver acquisito XX consensi al trattamento dei dati effettuato attraverso il dossier sanitario "a fronte di soli XX dinieghi".

In relazione alle risultanze della predetta attività istruttoria, l'Ufficio, con nota del XX (prot. n. XX), ha notificato all'Azienda Ospedaliero Universitaria Careggi, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'articolo 58, par. 2, del Regolamento, invitando il predetto titolare a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24/11/1981).

In particolare, nella predetta nota l'Ufficio ha evidenziato che la configurazione del dossier sanitario effettuata dall'Azienda è stata posta in essere in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento e dell'art. 75 del Codice e delle citate Linee guida. La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 4, lett. a) e par. 5, lett. a) del Regolamento.

Con nota del XX, l'Azienda ha inviato gli scritti difensivi, ribadendo quanto già rappresentato in atti e evidenziando, in particolare, che:

a partire dal XX, il Progetto "Archicare" -avviato nel gennaio 1996 al fine di consentire la dematerializzazione e l'informatizzazione della cartella clinica della sola unità operativa di tossicologia-, veniva replicato in altre unità operative e "nessun ulteriore dato diverso da quelli relativi al singolo evento clinico veniva importato né, tantomeno, reso visibile/accessibile";

a decorrere dal XX, la cartella è stata integrata con alcune ulteriori informazioni (nel XX in relazione alla cartella "XX" con i riferimenti alle lettere al curante e nel XX in relazione alla cartella "XX" con i riferimenti delle relazioni di degenza)" e che le

informazioni ivi accessibili "configuravano un trattamento sussumibile nell'ambito della disciplina relativa al dossier sanitario";

"La genesi, per così dire esperienziale e sperimentale, dello strumento approntato, dunque, unitamente al convincimento che esso non avesse l'ambizione né la finalità di creare un esteso e completo dossier - come propriamente descritto nelle citate Linee Guida del 2015 – ha portato gli sviluppatori e non ritenere, in assoluta buona fede e correttezza, che le cartelle "XX" e "XX" potessero essere attratte in siffatta disciplina e regolamentazione";

"Pur non consentendo [lo strumento implementato] un ampio accesso alla documentazione sanitaria (come accadrebbe in un Dossier propriamente qualificato e inteso) la possibilità di visualizzazione di dati, anche storici, relativi a pregressi e singoli eventi clinici verificatisi nella medesima Azienda, porta all'attrazione di tali trattamenti nell'ambito della disciplina di cui alle citate Linee Guida".

L'Azienda ha inoltre chiarito che il numero dei pazienti potenzialmente interessati dal contestato trattamento è pari a XX diversamente da quanto dichiarato in sede ispettiva di un numero pari a XX pazienti, attualmente registrati negli applicativi "Archicare" ciò in quanto "solo quando, in occasione di un episodio di ricovero o di prestazione ambulatoriale, viene richiesta una consulenza ad altra SOD ovvero per lo stesso paziente vengono predisposte lettere al curante, la cartella clinica di riferimento risulta, con le limitazioni sopra descritte, visibile a SOD diverse da quella presso la quale il paziente è curato. In tutte le altre ipotesi in cui non si verificano richieste "esterne" alla SOD, per l'effetto, non trova configurazione alcun trattamento assimilabile al dossier. Alla luce di questa doverosa precisazione, dal numero di pazienti sopra indicato devono essere espunti, quindi: i) quelli che hanno cartelle, sia di degenza che di ambulatorio, appartenenti ad una singola SOD; ii) quelli che non hanno lettere al curante. Il risultato di tale operazione consente di quantificare il numero dei pazienti, potenzialmente interessati dal contestato trattamento, in XX. Dato sensibilmente inferiore a quello rilevato".

L'Azienda ha poi ripercorso tutte le azioni tempestivamente poste in essere per conformare i trattamenti al quadro normativo di riferimento cooperando "attivamente con l'Autorità garantendo ampia disponibilità e capacità di immediata risposta in relazione alle evidenze da quest'ultima sollevate" (cfr. lettere del XX, XX e le memorie difensive).

L'Azienda ha inoltre chiarito, con riferimento alla "attribuzione di profili di abilitazione e autorizzazione al dossier differenziati in ordine alle diverse mansioni svolte e alle diverse e connesse attività di trattamento effettuate", che:

l'unico con privilegi di "medico super user" è il "Responsabile unico del progetto". […] Gli ulteriori profili attivati, […], avranno quindi limitazioni di accesso con limitate facoltà di consultazione […] cui vengono attribuite le sole funzioni necessarie allo svolgimento della propria attività";

"Il Responsabile unico del progetto, infatti, abilita all'interno di ogni SOD un "Amministratore Locale (AL)" (Responsabile medico della SOD) che, a sua volta, abilita il "Coordinatore Infermieristico (CI)" i quali provvedono all'attivazione delle nuove utenze, ciascuno per il profilo di competenza: "AL" per il personale medico e "CI" per il personale infermieristico";

"l'Amministratore locale definisce il periodo di validità dello stesso parametrandolo, sulla base di quanto rilevato dall'Ufficio del personale, alla durata del contratto ovvero, in relazione a specifiche figure professionali mediche (es. specializzandi, ritualmente nominati) per un periodo di tempo inferiore e ciò al fine di verificare costantemente le abilitazioni";

Con riferimento agli elementi rilevanti ai sensi dell'art. 83, par. 2 del Regolamento, l'Azienda ha dichiarato che:

"In merito agli interventi correttivi tempestivamente adottati […] si ritiene degna di nota l'implementazione di un sistema di gestione dei consensi totalmente informatizzato e conforme tanto alla normativa posta a tutela degli interessati con riguardo al trattamento dei dati personali, quanto ai recenti interventi normativi in tema di digitalizzazione della PA […]";

"L'intensa attività di aggiornamento condotta dall'Azienda sulla propria organizzazione, ha portato a una sostanziale conformità alla normativa applicabile in relazione ai trattamenti effettuati nell'ambito del dossier sanitario";

la totale buona fede e, quindi, un comportamento meramente colposo nella gestione delle attività di trattamento descritte, e importanti fattori depongono circa un'assenza di pregiudizio sui diritti e le libertà degli interessati quali: nessuna segnalazione ricevuta né alcun reclamo né, più in generale, alcuna pretesa risarcitoria dagli interessati;

"Pur consapevole della contestata lacuna informativa rilevata dall'Autorità in occasione dell'accertamento ispettivo, […] sul proprio sito istituzionale era presente e raggiungibile, da parte degli interessati, un'informativa relativa al Dossier Sanitario, oggi aggiornata";

"[…] ha ricevuto e correttamente gestito un'unica istanza di accesso ai dati trattati attraverso gli applicativi indicati, […] Le misure di sicurezza presenti, già all'epoca, hanno consentito di dare puntuale riscontro all'istante comunicando i log delle utenze che avevano effettuato l'accesso senza che ciò sfociasse in alcun contenzioso";

"Le tipologie di informazioni accessibili, rispetto a quelle ordinariamente consentite da un sistema di dossier sanitario, sono di fatto limitate a informazioni su ricovero e diagnosi di uscita, lettera di dimissione, lettera al curante per alcuni percorsi ambulatoriali: una minima parte, quindi, rispetto ai sistemi di dossier attenzionati dall'Autorità nei citati provvedimenti, Non sono accessibili, ad esempio, le cartelle cliniche e le cartelle ambulatoriali comprensive delle varie anamnesi"

"gli accessi alle informazioni assimilabili al dossier possono essere effettuati unicamente dal personale con profilo medico poiché il personale infermieristico, pur autorizzato, ha la possibilità di effettuare l'accesso unicamente alle informazioni trattate all'interno della SOD di appartenenza (e non, quindi, con accessi trasversali e orizzontali)".

In data XX, si è svolta l'audizione richiesta dall'Azienda, nella quale quest'ultima ad integrazione di quanto già ampiamente rappresentato ha dichiarato che:

"è stato individuato un parametro temporale di accesso al dossier individuato in 10 anni. Pertanto, i documenti sanitari relativi a prestazioni erogate oltre tale periodo non saranno visibili attraverso il dossier";

"l'investimento effettuato sulla formazione del personale su tali temi che è stato prontamente attivato a gennaio e i cui corsi sono stati già seguiti, con profitto, dal 25 % del personale destinatario degli stessi. Le interlocuzioni con i dipendenti mostrano un significativo interesse e coinvolgimento degli stessi su tali materie";

"Con riferimento ai profili di accesso, […] solamente i medici che sono coinvolti nel percorso di cura dell'interessato possono accedere ai sistemi informativi riconducibili al dossier sanitario";

"già alla data degli accertamenti ispettivi, tramite il dossier non è possibile accedere alla cartella clinica, ma solo alla lettera di dimissione, alla lettura curante e all'informazione relativa alla diagnosi di dimissione (non si accede ad esempio alla anamnesi del paziente".

L'Azienda ha inoltre prodotto una nota indirizzata al "personale sanitario titolato ad accedere agli applicativi XX e XX", in cui questi ultimi sono informati che "riceveranno un convocazione nella sezione del portale del dipendente […]" al fine di svolgere uno specifico corso di formazione obbligatorio sul "Dossier sanitario elettronico" della durata di 2 ore (nota del XX) e chiesto di "procedere all'archiviazione del procedimento amministrativo e, in subordine, pur senza riconoscere la fondatezza delle contestazioni, l'applicazione di una sanzione nella minore entità possibile".

Con nota dell'XX, l'Azienda ha inviato note integrative in relazione al procedimento avviato dal Dipartimento, nelle quali ha in particolare precisato di aver condotto delle verifiche e dei test sulla visibilità dei dati oggetto di trattamento tramite il dossier sanitario, simulando due distinti accessi, il primo "con il profilo medico appartenente alla medesima SOD o afferente al percorso di cura del paziente con consenso prestato alla costituzione del dossier e all'implementazione con dati pregressi", il secondo "con profilo medico non appartenente alla medesima SOD o afferente al percorso di cura del paziente con consenso prestato alla costituzione del dossier e all'implementazione con dati pregressi. Al riguardo, è stato di conseguenza dichiarato che "[…] il personale con profilo diverso da quello medico non ha alcuna visibilità dei dati relativi ai trattamenti afferenti al DSE".

Nello specifico, è emerso che il medico che ha in carico ambulatoriale il paziente, che ha prestato il consenso al dossier sanitario, può visualizzare la storia clinica dello stesso e accedere ai referti strumentali relativi a tutte le Unità organizzative (SOD).

È inoltre emerso che il profilo medico appartenente alla SOD nella quale il paziente è attualmente ricoverato e che ha prestato il consenso al dossier sanitario, ha accesso alla storia clinica del paziente estesa a tutte le SOD, potendo quest'ultimo accedere alle informazioni relative a tutti i ricoveri intercorsi presso l'Azienda e alle informazioni relative ai referti strumentali elaborati da tutti i reparti della Azienda medesima.

In relazione al profilo medico che non ha in carico ambulatoriale il paziente che ha prestato il consenso al dossier sanitario la "Ricerca della storia clinica del paziente [è] limitata alla propria SOD: il medico non può accedere alla storia clinica estesa a tutte le SOD ([il campo] "Tutte" non appare)".

In particolare, è stato dichiarato e documentato che "Il medico di SOD diversa da quella con in cura il paziente non ha la possibilità di accedere ad alcuna informazione contenuta nella cartelle ambulatoriale del paziente (e di conseguenza […] ai referti strumentali ad esempio)".

In relazione ai pazienti ricoverati è emerso che il "Profilo medico di una SOD diversa da quella nella quale si trova ricoverato attualmente il paziente (consenso DSE) non può accedere alle informazioni relative alla storia clinica del paziente relativa ad altre unità organizzative".

È pertanto stato documentato che "il medico di SOD diversa da quella con in cura il paziente non ha la possibilità di accedere ad alcuna informazione contenuta nella cartella del paziente (e di conseguenza l'accesso ai referti strumentali, ad esempio)".

2. Esito dell'attività istruttoria.

In via preliminare, si rappresenta che il trattamento di dati personali deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali e, in particolare, delle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, il "Regolamento") e del d.lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali – di seguito, il "Codice").

Con particolare riferimento alla questione in esame, si evidenzia che i dati personali devono essere "trattati in modo lecito corretto e trasparente" (principio di "liceità, correttezza e trasparenza" e "in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (principio di "integrità e riservatezza")" (art. 5, par. 1, lett. a) e f) del Regolamento).

I dati inoltre devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità e comunque, "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (principi della limitazione della finalità e di minimizzazione dei dati - art. 5, par. 1, lett. b) e c) del Regolamento).

Il Regolamento prevede poi che il titolare del trattamento metta in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", tenendo conto, tra l'altro, "della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 del Regolamento).

Tenendo conto tra l'altro della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento deve poi mettere in atto misure tecniche e organizzative

adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione e a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (art. 25 del Regolamento).

Con riferimento ai trattamenti oggetto del citato accertamento ispettivo, il Garante ha adottato le "Linee guida in materia di Dossier sanitario - 4 giugno 2015" (Provvedimento del 4.6.2015, pubblicato in G.U. 164 del 17 luglio 2015, consultabile su www.gpdp.it doc web n. 4084632), nelle quali sono state individuate un primo quadro di cautele, al fine di delineare specifiche garanzie e responsabilità, nonché misure e accorgimenti necessari ed opportuni da porre a garanzia dei cittadini, in relazione ai trattamenti di dati sanitari che li riguardano, che, al pari degli altri provvedimenti dell'Autorità, continuano ad applicarsi anche dopo la piena applicazione del Regolamento, in quanto compatibili con lo stesso (art. 22, comma 4, d.lgs n. 101/2018).

Nelle richiamate linee guida del 2015, il Garante ha specificato che il dossier sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo.

All'interessato, infatti, 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. Ciò significa che qualora l'interessato non manifesti il suo 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 (es. raccolta dell'anamnesi, 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 si è rivolto presso quella struttura l'interessato 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).

In seguito alla piena applicazione del Regolamento, con il provvedimento del 7 marzo 2019, il Garante ha individuato- a titolo esemplificativo- alcuni trattamenti in ambito sanitario che richiedono il consenso esplicito dell'interessato (art. 9, par. 2, lett. a) del Regolamento), tra i quali sono stati annoverati anche quelli effettuati attraverso il dossier sanitario (doc. web n. 9091942).

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.

In particolare, nell'informativa al dossier deve essere evidenziata l'intenzione del titolare del trattamento 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.

L'informativa deve indicare tra l'altro anche le modalità attraverso le quali rivolgersi al titolare per esercitare i propri diritti di, come pure quelle per revocare il consenso all'implementazione del dossier sanitario, per esercitare la facoltà di oscurare alcuni eventi clinici che lo riguardano e per visionare gli accessi che sono stati effettuati al dossier sanitario (cfr. successivo punto 2.3 e 2.4)

Una specifica menzione deve essere prevista nell'informativa qualora il titolare del trattamento intenda rendere accessibili mediante il dossier anche i dati soggetti a maggiore tutela dell'anonimato, ovvero le informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale (ad es., prestazioni rese a persone sieropositive o che fanno uso di sostanze stupefacenti, di sostanze psicotrope).

Un'importante garanzia a tutela della riservatezza dell'interessato riconosciuta nelle richiamate Linee guida consiste nella possibilità che lo stesso decida di oscurare taluni dati o documenti sanitari consultabili tramite tale strumento (par. 5.1). Ciò in analogia a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di alcuni eventi sanitari che lo riguardano. Ciò, anche nel rispetto della legittima volontà dell'interessato di richiedere il parere di un altro specialista senza che quest'ultimo possa essere influenzato da quanto già espresso da un collega.

Ferma restando, infatti, l'indubbia utilità di un dossier sanitario il più possibile completo, il titolare del trattamento deve garantire la possibilità per l'interessato di non far confluire in esso alcune informazioni sanitarie. Al riguardo, si evidenzia che di per sé il dossier sanitario costituisce uno strumento informativo incompleto. Indipendentemente dalle ipotesi di oscuramento, infatti, il dossier include solo le informazioni cliniche derivanti dagli accessi del paziente nella struttura sanitaria che utilizza il dossier e non anche quelle relative agli accessi effettuati presso altre strutture pubbliche e private.

È, inoltre, importante evidenziare che i dossier sanitari non certificano lo stato di salute dei pazienti, in quanto consistono in strumenti che possono aiutare il clinico ad inquadrare meglio e più rapidamente lo stato di salute di questi, nel rispetto del diritto dovere del medico di effettuare gli accertamenti che riterrà -anche deontologicamente- più opportuni.

L'"oscuramento" dell'evento clinico (revocabile nel tempo) deve avvenire con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").

Il titolare del trattamento è tenuto ad informare i soggetti abilitati ad accedere ai dossier in ordine alla possibilità che gli stessi possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento.

Nel caso in cui l'interessato richieda l'oscuramento delle informazioni e/o dei documenti oggetto dello stesso, questi restano comunque disponibili al professionista sanitario o alla struttura interna al titolare che li ha raccolti o elaborati (ad es., referto accessibile tramite dossier da parte del professionista, che lo ha redatto, cartella clinica accessibile da parte del reparto di ricovero). La documentazione clinica relativa all'evento oscurato deve essere comunque conservata dal titolare del trattamento in conformità a quanto previsto dalla normativa di settore.

Nelle richiamate Linee guida il Garante ha prescritto che i titolari del trattamento 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, nonché della data e dell'ora dello stesso. Di tale diritto esercitabile dagli interessati devono essere opportunamente informati anche i soggetti autorizzati ad accedere al dossier sanitario.

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 complessità, 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 è di trenta giorni dal ricevimento della richiesta medesima.

Nelle suddette Linee guida il Garante, al fine di scongiurare il rischio di un accesso alle informazioni trattate mediante il dossier sanitario da parte di soggetti non autorizzati o di comunicazione a terzi di dati sanitari da parte di soggetti a ciò abilitati, ha specificamente chiesto al titolare del trattamento di porre particolare attenzione nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati, dovendo essere limitato l'accesso al dossier al solo personale sanitario che interviene nel processo di cura del paziente ed essere adottate modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria.

A tal fine, nelle predette Linee guida, il Garante ha indicato ai titolari del trattamento di 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, pertanto, limitato al solo personale sanitario che interviene nel tempo nel processo di cura del paziente. Ciò significa che deve essere consentito l'accesso solo al personale che a vario titolo interviene nel processo di cura. 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.

Nelle predette Linee guida, il Garante ha ritenuto che "il titolare del trattamento deve mettere in opera sistemi per il controllo degli accessi anche al database e per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, attraverso l'utilizzo di indicatori di anomalie (c.d. alert) utili per orientare successivi interventi di audit. Il titolare deve prefigurare, quindi, l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento (es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi)" (punto 7, lett. b).

Alla luce di quanto emerso negli accertamenti ispettivi e negli ulteriori atti istruttori, si rileva che l'Azienda non acquisiva il consenso informato degli interessati in merito allo specifico trattamento dei dati personali effettuato attraverso il dossier sanitario, neanche con riferimento ai dati soggetti a maggior tutela, e infatti solo dopo l'intervento dell'Ufficio, ha iniziato -nel mese di XX - a fornire le informazioni di cui all'art. 13 del Regolamento in merito ai predetti trattamenti e ad acquisire i richiesti consensi e a consentire agli interessati l'eventuale revoca. Ciò stante, si ritiene accertato che la configurazione del dossier sanitario sia stata effettuata dall'Azienda, come dimostrato dai fatti in esame, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e 9 e 25 del Regolamento e dell'art. 75 del Codice e delle Linee guida sopra richiamate.

Si prende in ogni caso atto che l'Azienda, solo a seguito dell'accertamento ispettivo, ha posto in essere specifiche misure per conformare i trattamenti al richiamato quadro normativo applicabile, prevedendo in particolare:

- l'aggiornamento delle informazioni rese ai sensi dell'art. 13 del Regolamento in relazione al trattamento effettuato tramite il Dossier Sanitario con puntuale descrizione dei trattamenti effettuati che rientrano nel perimetro di applicazione delle Linee Guida del Garante (cit.);

- l'aggiornamento della modulistica necessaria per l'acquisizione dei consensi utili per l'istituzione e la gestione del Dossier Sanitario:

- la predisposizione di una procedura informatica idonea a acquisire i consensi per l'attivazione e la gestione del dossier sanitario. In particolare: "il personale impegnato nell'accettazione e identificazione del paziente (effettuata tramite Tessera Sanitaria), richiamando espressamente l'informativa di cui sopra e rendendola facilmente accessibile ai pazienti (sia mediante esposizione presso i punti di accettazione sia rinviando al sito istituzionale) richiede all'interessato un numero telefonico personale di cui abbia immediata disponibilità. Il sistema informatico, per ogni consenso richiesto (n. 3 consensi per: i) attivazione Dossier, ii) acquisizione eventi pregressi, iii) inserimenti dati "maggior tutela") genera un codice OTP che l'interessato deve prontamente comunicare per manifestare il proprio consenso. Al fine di garantire piena applicazione e ove l'interessato non disponga di un numero personale, gli operatori consentiranno, comunque, la manifestazione dei consensi su modulistica cartacea".

L'Azienda ha inoltre confermato di aver rettificato altresì i modelli di informativa e consenso in uso, eliminando l'acquisizione del consenso degli interessati per finalità di cura tenuto conto che al riguardo, il Garante ha più volte evidenziato che, a seguito della piena applicazione del Regolamento, diversamente dal passato, 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 come quella in esame (cfr. provvedimento del 7 marzo 2020, doc. web n. 9091942). Sulla base dell'art. 9, par. 2, lett. h) e par. 3 del Regolamento, sono consentiti infatti i trattamenti per "finalità di cura" 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.

Fermo restando che alla data dell'attività ispettiva, non essendo stata fornita alcuna informativa agli interessati, gli stessi non erano a conoscenza dell'esistenza di un trattamento che li riguardasse, è emerso che l'interessato non poteva richiedere l'oscuramento di un singolo documento sanitario all'interno del dossier, ma solo l'oscuramento dell'intera cartella sanitaria; di tale facoltà il paziente non veniva comunque specificamente informato. Non erano dunque previsti oscuramenti parziali dei documenti di cui si compone la cartella di degenza ad eccezione della relazione di degenza.

Ciò stante, risulta accertato che la configurazione del dossier sanitario effettuata dall'Azienda, come dimostrato dai fatti in esame, è stata effettuata in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) del Regolamento e delle Linee guida sopra richiamate.

Si prende in ogni caso atto delle misure implementate dall'Azienda relative all'aggiornamento delle procedure e all'adozione di una specifica modulistica per la richiesta di oscuramento di un singolo documento sanitario all'interno del dossier e per la relativa revoca (cfr. note del XX, del XX e memorie difensive).

Nel ribadire che, alla data dell'attività ispettiva, non essendo stata fornita alcuna informativa agli interessati, gli stessi non erano a conoscenza dell'esistenza di un trattamento che li riguardasse, è emerso che l'interessato non era stato neppure informato in merito al diritto di conoscere gli accessi che sono stati effettuati sul suo dossier sanitario.

Ciò stante, risulta accertato che la configurazione del dossier sanitario, come dimostrato dai fatti in esame, è stata effettuata dall'Azienda in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) del Regolamento e delle Linee guida sopra richiamate.

Con riferimento a tale diritto con nota del XX, l'Azienda ha inviato la specifica modulistica messa a disposizione dei pazienti per l'esercizio dei diritti relativi ai trattamenti effettuati attraverso il dossier sanitario (cfr. moduli da 5 ad 8 della nota del XX).

Con specifico riferimento ai profili di autorizzazione per l'accesso al dossier sanitario è emerso che essi non risultavano conformi a quanto indicato nelle Linee guida del Garante del 2015 e al principio di liceità del trattamento. Infatti, il medico, con riferimento a pazienti ricoverati o che avevano una cartella ambulatoriale in una unità operativa a cui lo stesso è abilitato, poteva effettuare una ricerca sullo storico del paziente che gli restituiva l'elenco dei ricoveri e delle lettere al curante (a partire dal 1996 per l'unita di tossicologia) effettuati anche in unità operative diverse da quelle a cui lo stesso era abilitato. In tal caso, il predetto medico dopo aver dichiarato nel sistema di aver acquisito il consenso verbale del paziente (non comprovato considerato che il paziente non era a conoscenza dell'esistenza di un dossier sanitario), poteva accedere, per ciascuna cartella ambulatoriale o di ricovero sopra indicati, solo alla lettera al curante o alla relazione di degenza.

Pertanto, difformemente a quanto indicato nelle citate Linee guida e al principio di liceità del trattamento, l'accesso al dossier non era limitato al solo personale sanitario che verosimilmente poteva interviene nel tempo nel processo di cura del paziente, ovvero che, sulla base delle prestazioni erogate e dei percorsi clinici attivati, poteva effettivamente essere coinvolto nel percorso di cura del paziente.

Tutto ciò premesso, l'Azienda non ha previsto in modo completo l'attribuzione di profili di abilitazione e autorizzazione al dossier differenziati in ordine alle diverse mansioni svolte e alle diverse e connesse attività di trattamento effettuate dal personale sanitario, in conformità a quanto indicato nelle citate Linee guida e ai principi di protezione dei dati fin dalla progettazione di cui all'art. 25 del Regolamento.

In base al principio di "protezione dei dati fin dalla progettazione" (art. 25, par. 1, del Regolamento), il titolare infatti deve adottare misure tecniche e organizzative adeguate ad attuare in maniera efficace i principi di protezione dei dati (art. 5 del Regolamento) e integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati.

Con la nota del XX, l'Azienda ha dichiarato di aver predisposto le policy per le attività di provisionig e deprovisioning degli accessi e contestuale verifica della c.d. profondità dell'accesso (all. 12), con riferimento alle quali non risultava ancora chiaro come sia stato garantito che al professionista sanitario siano attribuiti profili di abilitazione e autorizzazione al dossier differenziati in ordine alle diverse mansioni svolte e alle diverse e connesse attività di trattamento effettuate.

Solo attraverso gli interventi correttivi documentati nel mese di XX l'accesso allo storico dei documenti sanitari attraverso il dossier sanitario è stato consentito al solo personale medico che ha in cura l'interessato. Ciò stante, fermi i chiarimenti da ultimo forniti e documentati con la nota dell'XX al fine di garantire che al professionista sanitario siano attribuiti profili di abilitazione e autorizzazione al dossier differenziati in ordine alle diverse mansioni svolte e alle diverse e connesse attività di trattamento effettuate, risulta accertato che, all'epoca dell'accertamento ispettivo e come dimostrato dai fatti in esame, la configurazione del dossier sanitario effettuata dall'Azienda è stata effettuata in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento e delle citate Linee guida.

Secondo quanto dichiarato in atti, si rileva inoltre che l'Azienda, non aveva -alla data dell'accertamento ispettivo- adottato -come indicato dalle citate Linee guida- un sistema per il rilevamento automatico di eventuali anomalie che possano configurare trattamenti illeciti, ovvero l'utilizzo di indicatori di anomalie (c.d. alert) volti ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti autorizzati al trattamento (es. numero degli accessi eseguiti, tipologia o ambito temporale degli stessi), utili per orientare successivi interventi di audit.

Ciò stante risulta accertato che la configurazione del dossier sanitario effettuata da codesta Azienda, come dimostrato dai fatti in esame, è stata effettuata in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento e delle citate Linee guida.

Si prende atto delle misure che l'Azienda ha dichiarato di voler implementare in termini di controlli a campione sugli accessi effettuati al dossier sanitario che dovrebbero iniziare nel mese di XX unitamente a specifici corsi di formazione che l'Azienda si è impegnata a svolgere e che ha effettivamente svolto (cfr. verbale di audizione del XX).

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria - e considerato che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante" - si rappresenta che gli elementi forniti dal titolare del trattamento nelle memorie difensive e nelle successive note integrative, relative al richiamato procedimento non consentono

di superare i rilievi notificati dall'Ufficio con gli atti di avvio del procedimento per l'adozione dei provvedimenti correttivi e sanzionatori, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dall'Azienda Ospedaliero Universitaria Careggi con riferimento al procedimento avviato a seguito degli accertamenti ispettivi e della notifica di violazione, nei termini di cui in motivazione, in particolare, per aver trattato dati personali attraverso il dossier sanitario in violazione degli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento, dell'art. 75 del Codice e delle citate Linee guida.

In tale quadro, avendo l'Azienda posto in essere le misure correttive necessarie a conformare il trattamento dei dati personali tramite il dossier sanitario al quadro normativo vigente, sopra richiamato, la condotta contestata ha cessato di produrre i suoi effetti e pertanto non ricorrono i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

4. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

La violazione degli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento e dell'art. 75 del Codice e delle citate Linee guida, causata dalla condotta dell'Azienda Ospedaliero Universitaria Careggi è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4 e 5, del Regolamento.

Si consideri che il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Ritenuto di dover applicare il par. 3 dell'art. 83 del Regolamento laddove prevede che "se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Alla luce di quanto sopra illustrato e, in particolare, della categoria di dati personali interessata dalla violazione che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, del numero dei soggetti interessati (XX pazienti) i cui dati sono stati trattati tramite il dossier sanitario in violazione delle disposizioni sopra richiamate, della durata della violazione (dal 2011-2025), nonché della circostanza che la collaborazione dell'Azienda si è tradotta nell'adozione di misure, comunque, indilazionabili per porre fine all'accesso indiscriminato al dossier si ritiene che il livello di gravità della violazione commessa dall'Azienda sia alto (cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60).

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini dell'applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione, tenuto conto che la sanzione deve essere "in ogni singolo caso effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nell'ipotesi in esame, sono state tenute in considerazione le circostanze sotto riportate:

- la natura dei dati, il numero degli interessati e la durata della violazione (art. 83, par. 2, lett. a) del Regolamento);

- le misure implementate dall'Azienda -solo nel XX a seguito dell'accertamento ispettivo del Garante- per conformare il trattamento dei dati personali dei pazienti effettuato attraverso il dossier sanitario al quadro normativo vigente anche al fine di tutelare i diritti e le liberta degli interessati (art. 83, par. 2, lett. c) del Regolamento);

- il Garante ha preso conoscenza delle violazioni a seguito degli accertamenti ispettivi svolti (art. 83, par. 2, lett. h) del Regolamento);

- l'Azienda non è destinataria di precedenti provvedimenti prescrittivi o sanzionatori relativamente allo stesso oggetto ed ha collaborato nel corso dell'attività istruttoria che l'ha visto coinvolta (art. 83, par. 2, lett. e) e f) del Regolamento);

- la circostanza che non erano accessibili, le cartelle cliniche e quelle ambulatoriali comprensive delle varie anamnesi ma solo informazioni su ricovero e diagnosi di uscita, lettera di dimissione, lettera al curante per alcuni percorsi ambulatoriali (art. 83, par. 2, lett. k) del Regolamento);

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti della Azienda la sanzione amministrativa del pagamento di una somma pari ad euro 20.000,00 (ventimila/00).

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione della gravità della condotta contestata che coinvolge la disciplina sulla protezione dei dati personali di un numero elevato di interessati e della circostanza che tali trattamenti sono stati oggetto di uno specifico provvedimento generale adottato dal Garante fin dal 2015.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato, descritti, dall'Azienda Ospedaliero Universitaria Careggi per la violazione degli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento e dell'art. 75 del Codice e delle citate Linee guida nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Azienda Ospedaliero Universitaria Careggi, con sede in Largo Brambilla, 3, 50134, Firenze, C.F. /P.IVA 04612750481, di pagare la somma di euro 20.000,00 (ventimila/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento.

INGIUNGE

alla predetta Azienda, di pagare la predetta somma di euro 20.000,00 (ventimila/00), secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981. Si rappresenta che ai sensi dell'art. 166, comma 8 del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento -sempre secondo le modalità indicate in allegato- di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 del 1° settembre 2011 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento;

Ai sensi dell'art. 78 del Regolamento, nonché degli articoli 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 individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 4 agosto 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Fanizza