Provvedimento correttivo e sanzionatorio nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona - 23 gennaio 2020 [9269629]

VEDI ANCHE Newsletter del 18 febbraio 2020

[doc. web n. 9269629]

Provvedimento correttivo e sanzionatorio nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona - 23 gennaio 2020

Registro dei provvedimenti
n. 18 del 23 gennaio 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla 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 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");

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 la dott.ssa Licia Califano;

PREMESSO

1. La violazione dei dati personali.

Nel mese di maggio del 2019, l'Azienda Ospedaliero Universitaria Integrata di Verona (di seguito Azienda) ha inviato all'Autorità tre comunicazioni relative a violazioni di dati personali ai sensi dell'art. 33 del Regolamento, in relazione a quanto emerso nell'ambito

dei controlli, periodicamente effettuati dall'Azienda in materia di accessi ai dossier sanitari dei pazienti (comunicazioni del 6.5.2019- prot. n. 25344; del 9.5.2019- prot. n. 26161 e del 22.5.2019- prot. n. 28317).

Nella comunicazione del 6 maggio 2019, l'Azienda ha affermato di aver "riscontrato un accesso improprio a sei dossier di pazienti che sono al tempo stesso dipendenti aziendali nel ruolo di ostetriche" e che "non vi era motivo che un medico della (…) Unità Operativa (di Ostetricia e Ginecologia) compresa dunque la d.ssa titolare delle credenziali, facesse accesso ai dati clinici di pazienti non in carico, alcune delle quali per di più a casa in congedo per maternità al tempo dell'episodio, e che pertanto si è trattato di accessi impropri". Secondo quanto dichiarato, l'accesso è stato effettuato "con le credenziali di un medico dell'UOC di Ostetricia e Ginecologia" che, durante il turno notturno di guardia medica, "ha lasciato incustodita e accessibile la postazione pc in uso, consentendo ad altri di accedere ai dati sanitari delle sei ostetriche". L'Azienda ha dichiarato che ne sarebbe stata data tempestiva comunicazione alle interessate.

Nella comunicazione del 9 maggio 2019, l'Azienda ha dichiarato di aver "riscontrato un accesso improprio al dossier sanitario di sette pazienti che sono al tempo stesso dipendenti aziendali". Secondo quanto dichiarato, l'accesso è stato effettuato "da un tecnico sanitario di radiologia medica", al fine di "vedere come funzionava l'applicazione" e, in altri casi, mediante l'utilizzo delle credenziali di autenticazione dello stesso soggetto che aveva lasciato la propria postazione "incustodita e accessibile". L'Azienda ha indicato, nella predetta notificazione, che "verificati gli orari e le postazioni di lavoro nelle date citate, (…) non c'era nessuna esigenza ad accedere al dossier sanitario de pazienti-dipendenti segnalati";

Nella comunicazione del 22 maggio 2019, l'Azienda ha dichiarato che "un medico in formazione specialistica presso l'UOC di Neurologia B dell'Ospedale di Bogo di Roma" ha effettuato un "accesso improprio al dossier sanitario di alcuni pazienti che sono al tempo stesso dipendenti aziendali". Secondo quanto dichiarato in atti, in tre distinte fattispecie, l'accesso ha riguardato i dossier sanitari di colleghi neurologi non in cura presso il reparto di afferenza dello specializzando e che, secondo quanto indicato dal Direttore dell'UOC di Neurologia, non dovevano essere visionati dal tale soggetto. Tenuto conto delle circostanze, l'Azienda ha dichiarato "possibile che l'accesso sia stato dettato da mera curiosità" e ha dichiarato che ne sarebbe stata data tempestiva comunicazione agli interessati.

Nelle suddette notificazioni l'Azienda ha affermato di aver portato a conoscenza di tutto il personale, tramite il "Disciplinare tecnico sull'uso delle risorse informatiche aziendali" e le istruzioni presenti negli atti di designazione a incaricati/autorizzati al trattamento (ivi compresi i specializzandi), specifiche indicazioni in merito ai presupposti di liceità degli accessi al dossier sanitario aziendale (anche con specifico riferimento ai dossier sanitari di colleghi) e alle misure relative all'impostazione di un intervallo di timeout per la sessione dell'applicativo utilizzato per il dossier, che saranno ulteriormente e più dettagliatamente rinnovate al personale.

Con specifico riferimento ai fatti oggetto della comunicazione del 9 maggio 2019, l'Azienda ha dichiarato l'intenzione di implementare "ulteriori e più sofisticati filtri che permetteranno ai tecnici di radiologia di consultare i soli dati (immagini) necessari allo svolgimento dei propri compiti".

Nelle predette comunicazioni di violazioni l'Azienda ha dichiarato di aver avviato un procedimento disciplinare nei confronti dei dipendenti responsabili dei predetti accessi non autorizzati ai dossier sanitari (radiologia e neurologia) e di essere in fase di valutazione per una censura formale anche nei confronti del medico dell'UOC di Ostetricia e Ginecologia che, seppur in turno notturno di guardia, ha "contravvenuto a precise istruzioni aziendali".

L'Azienda ha, inoltre, affermato che, alla luce di tutti gli episodi oggetto delle predette notificazioni, "sarà attivato sull'applicativo che gestisce il dossier sanitario un disclaimer che, ogni qualvolta un operatore sanitario si accinga ad accedere alla documentazione sanitaria di un paziente che non è in carico all'Unità operativa di afferenza, gli ricorda che quell'accesso sarà tracciato e monitorato, elencando le regole essenziali che vi presiedono".

2. L'attività istruttoria.

In relazione alle predette comunicazioni di violazioni, l'Ufficio, con atto n. 25322/19 del 22 luglio 2019, con riferimento alle specifiche situazioni di illiceità in esso richiamate, ha notificato all'Azienda, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'articolo 58, paragrafo 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 l'Ufficio, nel predetto atto, ha disposto la riunione dei procedimenti istruttori relativi alle comunicazioni effettuate e ha ritenuto che le violazioni di dati personali notificate al Garante ai sensi dell'art. 33 del Regolamento, abbiano rilevato la sussistenza di elementi idonei a configurare da parte dell'Azienda le violazioni di cui agli artt. 5 e 9 del Regolamento, rappresentando che:

- con riferimento ai trattamenti oggetto di notificazione, 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), 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 predette 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;

- sulla base degli elementi acquisiti e della documentazione in atti, risulta accertato che personale sanitario dell'Azienda ha acceduto al dossier sanitario di pazienti che sono, al tempo stesso, dipendenti dell'Azienda e colleghi degli autori degli accessi in assenza di un idoneo presupposto giuridico, e -in taluni casi- ha lasciato incustodito il terminale in uso con tutte le proprie abilitazioni attive, rendendo possibile l'accesso da parte di terzi ai dossier sanitari dei pazienti dell'Azienda.

Con nota del 21 agosto 2019 (prot. n. 45332), l'Azienda ha fatto pervenire le proprie memorie difensive, in cui, in sintesi, è stato rappresentato che l'"(accesso a dossier sanitario di pazienti, che sono al tempo stesso dipendenti di questa Azienda, in assenza di idoneo presupposto giuridico) è da ascrivere, in tutte e tre le ipotesi in questione, a una condotta "infedele" di personale aziendale che ha agito in spregio a precise indicazioni impartite dal titolare del trattamento e alle regole stabilite per governare gli accessi all'archivio informatizzato dei dati di salute dei pazienti, tant'è che in due casi si è proceduto anche a inoltrare denuncia all'Autorità Giudiziaria competente nei confronti dei presunti colpevoli per il reato di cui all'art. 615-ter, codice penale".

In particolare, negli scritti difensivi, l'Azienda ha dichiarato che:

a) considerato il livello di rischio per i diritti e libertà degli interessati, ha notificato i predetti accessi all'Autorità e ha provveduto a darne comunicazione agli interessati;

b) gli interessati non hanno subito un danno di entità misurabile "potendosi ragionevolmente ascrivere a "mera curiosità" la motivazione che ha spinto gli autori degli accessi a effettuarli", come dimostrerebbe il fatto che gli accessi indebiti "sono stati scoperti all'esito di controlli effettuati dall'Azienda sull'uso dell'applicativo che gestisce il dossier sanitario dei pazienti, e non sulla base di segnalazioni provenienti dagli interessati", nonché dal fatto che, a fronte della comunicazione agli interessati di un accesso indebito al dossier sanitario, "solo quattro dipendenti sui diciannove notiziati (considerati tutti e tre i casi contestati) ha fatto domanda di conoscere quali documenti sanitari fossero stati oggetto di illecita presa visione"; al riguardo l'Azienda ha precisato che "in tre casi (dei diciannove anzidetti) all'accesso al dossier dei pazienti in questione non ha fatto seguito alcuna attività di presa visione di documenti clinici";

c) "quanto al carattere doloso o colposo della violazione (art. 83, par. 2, lett. b), RGPD), se da parte degli autori materiali il dolo non può essere messo in dubbio (compreso il caso notificato con la nota del 6 maggio 2019, dove è stato con ragionevole certezza accertato che l'accesso illecito è stato dolosamente commesso da ignoti sfruttando la postazione lasciata colposamente incustodita dalla d.ssa in turno notturno di guardia), valutata dal punto di vista dell'Azienda titolare del trattamento, ogni intenzionale lesione della riservatezza degli interessati va evidentemente esclusa, trovando difficile d'altro canto rinvenire negligenze o trascuratezze all'Azienda stessa direttamente imputabili, anche alla luce di quanto più sotto precisato";

d) per quanto riguarda le misure adottate dal titolare del trattamento per attenuare il danno subito dagli interessati (art. 83,

par. 2, lett. c) del Regolamento), l'Azienda "ha scoperto la violazione grazie ai controlli sistematici approntati, e ne ha fatto pronta denuncia" al Garante e "ha messo in atto misure correttive volte a ridurre ulteriormente le possibilità che si possa ripetere in futuro", impedendo "la progressione a un livello che poteva avere gravi ripercussioni nei confronti degli interessati";

e) "fin dall'emanazione, a cura di codesta Autorità, a giugno del 2015 delle nuove Linee guida in materia di dossier sanitario (…) l'Azienda ha tempestivamente assunto le misure, tecniche e organizzative, reputate necessarie per adeguarsi alle indicazioni del Garante" e "ha assunto ulteriori iniziative, anche informative", fra cui si segnalano:

- "l'inserimento sull'applicativo di gestione del dossier di una pagina di avvertimento che ora compare in automatico ogni qualvolta si consulti la documentazione clinica di paziente non in carico alla struttura di afferenza del sanitario che sta effettuando l'accesso, dove si segnala all'utente che l'accesso stesso sarà tracciato e monitorato, con indicazione delle conseguenze sanzionatorie a cui si va incontro in caso di accessi illeciti o comunque non giustificati da reali esigenze di lavoro"

- "l'invio a tutti i Direttori di Unità Operativa e a tutti i Coordinatori delle professioni sanitarie, che in Azienda rivestono il ruolo di delegati privacy" della "nota prot. n. 35475 del 26.06.2019, con la quale è stata ritrasmessa la circolare del 2016, che, nell'illustrare i contenuti delle sopra citate Linee guida in materia di dossier sanitario emanate da codesta Autorità il 4 giugno 2015, forniva puntuali istruzioni a proposito degli adempimenti da porre in essere al fine di adeguarvisi, anche per ciò che concerne i controlli sulla liceità degli accessi al dossier";

- la rinnovata definizione delle "regole per il corretto trattamento dei dati personali contenuti nel dossier sanitario, con particolare riferimento all'accesso a documentazione clinica di pazienti non in carico per cui è richiesta una specifica motivazione da scegliere in un menù a tendina che riproduce quelle più frequentemente utilizzate, oppure da digitare in un campo note libero";

- la prossima attivazione di "nuove regole che permetteranno il raffinamento dell'algoritmo di determinazione dello stato di "paziente in carico", che finora ha rappresentato il discrimine per l'accesso diretto, con o senza motivazione, alla storia clinica dei pazienti da parte degli operatori coinvolti a vario titolo nel processo di cura degli stessi", al fine di "limitare temporalmente ai sistemi integrati l'accesso al dossier dei soli pazienti inseriti in una lista di lavoro (prenotazione da CUP, accesso a Pronto Soccorso, ricovero, etc.), e dunque tutti presi in carico dalle strutture che a vario titolo li devono trattare; per la sola categoria dei medici, stante l'esigenza di garantire il "diritto alla salute", a fronte di una richiesta di accesso al di fuori del limite temporale predefinito, l'accesso stesso sarà comunque consentito previa motivazione, soggetta a verifica. Riducendo in tal modo gli accessi a dossier con motivazione, per i quali il sistema non ha riconosciuto la presa in carico del paziente, saranno migliorate l'efficacia e l'efficienza dei controlli, che andranno a monitorare solamente gli accessi potenzialmente inappropriati, limitando il numero dei cd. "falsi positivi".

- con specifico riferimento alla categoria dei tecnici sanitari di radiologia medica, uno dei quali è stato coinvolto nella violazione notificata il 09.05.2019, "le modifiche in via di realizzazione impediranno il verificarsi in futuro di episodi simili a quello di cui trattasi; finora infatti ai tecnici in questione era consentito, per permettere peraltro il corretto svolgimento del proprio lavoro secondo precise indicazioni della Direzione delle professioni sanitarie, di accedere al dossier dei pazienti inseriti nel sistema radiologico senza il filtro temporale, di prossima attivazione come detto, dell'iscrizione del paziente in una lista di lavoro alla data di esecuzione della prestazione, e quindi limitandosi a immettere la motivazione richiesta all'atto della chiamata di contesto dall'applicativo verticale in uso presso i servizi di radiologia. È in cantiere anche la creazione per i tecnici di radiologia di un profilo aggiuntivo che consentirà loro di accedere non all'intero dossier del paziente, ma solo ai documenti in esso inseriti che sono di stretto interesse per la loro attività (referti e immagini radiologiche): come già precisato in sede di notifica, trattasi di intervento particolarmente oneroso e di non immediata attuazione, perché fortemente impattante sul software di riferimento".

3. Esito dell'attività istruttoria.

Preso atto di quanto rappresentato dall'Azienda nelle memorie difensive, si osserva che:

1. come più volte affermato in atti, i 16 (sedici) accessi oggetto di istruttoria da parte dell'Ufficio del Garante non sono stati effettuati da parte del personale medico al fine di erogare prestazioni di cura agli interessati, ma per ragioni personali descritte dall'Azienda come "mera curiosità", in violazione degli artt. 5 e 9 del Regolamento;

2. le comunicazioni effettuate dall'Azienda hanno permesso di evidenziare che le misure adottate dalla stessa, con riferimento ai trattamenti effettuati attraverso il dossier sanitario aziendale, non hanno permesso di evitare la possibilità che il personale sanitario abilitato accedesse alla documentazione clinica di pazienti non in cura presso gli stessi, determinando un trattamento illecito dei dati personali riguardanti gli interessati, in violazione dell'art. 5 del Regolamento;

3. in particolare, l'Azienda ha adottato misure tecniche e organizzative che si sono rilevate non pienamente adeguate al fine di garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati come stabilito dall'art. 5, par. 1, lett. f), del Regolamento;

4. l'Azienda, in violazione dell'art. 5, par. 1, lett. f), del Regolamento cit., ha implementato le misure volte a limitare l'accesso al dossier sanitario dei pazienti solo al personale sanitario che li ha in cura in un determinato momento solo dopo aver accertato gli episodi oggetto delle predette comunicazioni (misure descritte nella precedente lettera e)), individuando delle soluzioni logico- informatiche che si basano, di fatto, sulle indicazioni già fornite dal Garante nelle citate Linee guida del 2015 (cfr. par. 6 delle citate Linee guida) e ribadite nei provvedimenti adottati dall'Autorità in materia sin dal 2013 e pubblicati sul sito del Garante (cfr. provvedimenti del 10.1.2013 -doc. web n. 2284708, del 3.7.2014 -doc. web n. 3325808, del 23.10.2014 -doc. web n. 3570631, del 18.12.2014 – doc. web n. 3725976, del 22.10.2015 -doc web n. 4449114 e del 22.6.2016 – doc. web n. 5410033). L'adozione preventiva di tali misure, anche alla luce dei principi di protezione dei dati fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default) contemplati all'art. 25 del Regolamento, avrebbe potuto impedire (o limitare) i predetti accessi non autorizzati ai dossier sanitari aziendali oggetto delle citate comunicazioni di violazioni effettuate dall'Azienda;

5. con specifico riferimento all'accesso ai dossier sanitari aziendali da parte dei tecnici sanitari di radiologia medica (cfr. violazione notificata il 09.05.2019), secondo quanto dichiarato in atti, non era stato individuato alcun "filtro temporale", né alcuna limitazione relativamente alla tipologia di dati o di documenti dagli stessi accessibili. In violazione dell'art. 5 del Regolamento, l'Azienda, solo a seguito dei fatti oggetto della comunicazione del 9 maggio 2019, ha quindi deciso di adottare misure (attualmente in corso di attuazione) volte a limitare l'accesso ai dossier sanitari dei pazienti presi in carico dai predetti tecnici attraverso l'individuazione di uno specifico "profilo" che consentirà agli stessi di accedere ai soli documenti necessari per lo svolgimento delle attività agli stessi attribuite. Al riguardo, il Garante, nelle predette Linee guida del 2015, aveva già indicato la necessità che il titolare del trattamento effettuasse 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. Spetta al titolare del trattamento valutare, infatti, in relazione ai diversi profili di autenticazione al dossier, se sia indispensabile che siano in concreto accessibili tutti i dati e i documenti presenti nello stesso o solo una parte di essi (cfr. punto 6 delle citate Linee guida).

4. 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 non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, 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 Integrata di Verona, nei termini di cui in motivazione, in particolare, per aver trattato dati personali in violazione dell'art. 5, par. 1, lett. f), del Regolamento.

5. Misure correttive.

Alla luce delle valutazioni sopra richiamate, si ritiene di dover ingiungere all'Azienda Ospedaliero Universitaria Integrata di Verona,

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, le seguenti misure correttive:

- entro il termine di giorni 90 dalla notifica del presente provvedimento, completare l'implementazione delle misure descritte nelle notificazioni inviate al Garante e negli scritti difensivi volte a migliorare le procedure di accesso ai dossier sanitari aziendali da parte del personale a ciò autorizzato.

6. 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 dell'art. 5, par. 1, lett. f), del Regolamento, causata dalla condotta posta in essere dall'Azienda, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 5, lett. a) del Regolamento.

Il Garante, ai sensi 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).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 85, par. 2, del Regolamento in relazione ai quali si osserva che:

- l'Autorità ha fornito specifiche indicazioni in merito all'applicazione della disciplina sulla protezione dei dati personali ai trattamenti effettuati attraverso i dossier sanitari aziendali già con le richiamate Linee guida del 2015 (art. 83, par. 2, lett. a) del Regolamento);

- l'Azienda ha deciso di implementare le misure volte a limitare l'accesso al dossier sanitario dei pazienti solo al personale sanitario che lo ha in cura in un determinato momento pe a individuare, in relazione ai diversi profili di autenticazione al dossier, i dati e i documenti di cui è indispensabile l'accesso solo dopo aver accertato gli episodi oggetto delle predette comunicazioni, attraverso soluzioni logico- informatiche già indicate dal Garante nelle citate Linee guida del 2015 (cfr. par. 6 delle citate Linee guida) e ribadite nei provvedimenti adottati dall'Autorità in materia sin dal 2013 e pubblicati sul sito del Garante (art. 83, par. 2, lett. c) e d) del Regolamento);

- seppure il numero degli interessati i cui dati sono stati oggetto di violazione non è particolarmente elevato (16 interessati) rispetto a quello totale degli assistiti dall'Azienda, analoghi accessi non autorizzati si sarebbero potuti verificare nei confronti di un numero ben maggiore di interessati, non avendo l'Azienda implementato, soprattutto con riferimento al personale radiologo, misure idonee a limitare l'accesso ai soli dossier dei pazienti effettivamente in cura e ai soli dati personali ritenuti necessari a garantire l'attività sanitaria prestata (art. 83, par. 2, lett. a) e d) del Regolamento);

- gli accessi non autorizzati oggetto delle predette notifiche hanno riguardato documentazione clinica contenente numerosi dati sulla salute degli interessati (art. 4, par. 1, n. 15 del Regolamento). Al riguardo, si deve considerare, inoltre, che i predetti accessi hanno avuto ad oggetto informazioni riconducibili alle categorie particolare di dati, consultabili attraverso un particolare strumento informativo che, per sua natura, è deputato a documentare la storia clinica di una persona, attraverso la raccolta della documentazione relativa a tutte le prestazioni sanitarie (referti, cartelle cliniche, verbali di pronto soccorso) erogate dall'Azienda allo stesso soggetto nel corso del tempo (in tal senso, cfr. anche le informazioni rese dall'Azienda sul dossier sanitario sul proprio sito web, https://www.aovr.veneto.it/informativa-sul-dossier-sanitario-elettronico). Gli accessi oggetto delle predette comunicazioni di violazione hanno riguardato, infatti, non solo singoli referti, ma l'"archivio informatico" che l'Azienda stessa definisce come strumento volto a garantire "una conoscenza approfondita della storia clinica" dell'interessato (cfr. Predette informazioni rese dall'Azienda) (art. 83, par. 2, lett. g) del Regolamento);

- pur considerando l'assenza di reclami presentati all'Autorità da parte degli interessati i cui dati sono stati oggetto di accesso non autorizzato, non è possibile escludere che gli stessi possano aver subito, o subiscano in futuro, conseguenze pregiudizievoli per l'effetto di tali condotte, soprattutto in considerazione del fatto che si tratta di soggetti vulnerabili in quanto sono state accedute informazioni relative al loro stato di salute e che, nella totalità dei casi, gli interessati sono

anche dei colleghi dei soggetti che hanno effettuato l'accesso;

- secondo quanto dichiarato dall'Azienda, le ragioni che hanno motivato i predetti accessi, sono riconducibili alla "mera curiosità" (art. 83, par. 2, lett. b) del Regolamento);

In relazione alla vicenda si prende favorevolmente atto che:

- sia stata la stessa Azienda sanitaria a comunicare al Garante i predetti accessi ai dossier sanitari aziendali, mediante tre comunicazioni di violazione di dati personali sopra evidenziate (art. 83, par. 2, lett. h), del Regolamento);

- gli accessi, oggetto delle richiamate comunicazioni di violazione, sono stati individuati dall'Azienda nell'ambito dei controlli periodicamente effettuati dalla stessa in materia di accessi ai dossier sanitari dei pazienti (art. 83, par. 2, lett. d) del Regolamento). I predetti accessi si riferiscono a condotte effettuate dai 3 ai 6 mesi antecedenti ai predetti controlli aziendali;

- l'Azienda abbia spontaneamente avviato una revisione delle specifiche tecniche e organizzative relative all'accesso ai dossier sanitari aziendali.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5, lett. a) del Regolamento, nella misura di euro 30.000 (trentamila) per la violazione dell'art. 5, par. 1, lett. f), del Regolamento quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019, anche in considerazione dell'invasività dei trattamenti illeciti contestati rispetto ai diritti fondamentali degli interessati, della tipologia di dati personali oggetto di illecito trattamento, delle carenze riscontrate in relazione alla sicurezza dei sistemi informativi dell'Azienda.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dall'Azienda Ospedaliero Universitaria Integrata di Verona, per la violazione dell'art. 5 par. 1, lett. f), del Regolamento nei termini di cui in motivazione.

INGIUNGE

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, all'Azienda Ospedaliero Universitaria Integrata di Verona entro il termine di giorni 90 dalla notifica del presente provvedimento, di completare l'implementazione delle misure descritte nelle notificazioni inviate al Garante e negli scritti difensivi, volte a migliorare le procedure di accesso ai dossier sanitari aziendali da parte del personale a ciò autorizzato.

Al riguardo, si richiede all'Azienda di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto sopra ingiunto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato, ai sensi dell'art. 157 del Codice, entro il termine di giorni 20 dalla scadenza del termine sopra indicato; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, paragrafo 5, del Regolamento.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Azienda Ospedaliero Universitaria Integrata di Verona, con sede legale in Verona (VR), Piazzale Aristide Stefani, 1 - C.F./P. IVA 0390142023, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 30.000,00 (trentamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento, secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981.

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 30.000,00 (trentamila), secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 23 gennaio 2020

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia