Privacy

Sanità digitale: un recente caso di data breach sanzionato dall'Autorità Garante

di **Franco Cardin**

Opportunità e rischi del processo di digitalizzazione in sanità

In diverse occasioni il Garante per la protezione dei dati personali, pur riconoscendo che il processo di digitalizzazione in sanità va senz'altro promosso - in quanto rappresenta un'opportunità non solo per migliorare l'efficacia delle prestazioni di cura, ma anche per garantire una maggiore efficienza del sistema sanitario nazionale - ha evidenziato la necessità che lo stesso sia governato con la massima attenzione in quanto coinvolge categorie particolari di dati personali tra le più delicate, quali sono quelli relativi allo stato di salute.

A questo proposito basti ricordare che nel 2009 l'Autorità Garante, preso atto del sempre più frequente utilizzo da parte delle aziende sanitarie delle tecnologie informatiche e telematiche, ha ritenuto necessario, nelle more di un opportuno e auspicato intervento normativo, individuare un primo quadro di regole, accorgimenti e cautele finalizzate a garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, adottando le *"Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario"*.

Successivamente, come è noto, le regole e le misure di sicurezza contenute nelle predette linee guida sono state recepite nel DPCM 29.09.2015, n. 178 *"Regolamento in materia di fascicolo sanitario elettronico"*, con il quale è stata data attuazione a quanto previsto dall'art. 12 della legge 221/2012.

Per quanto riguarda, in particolare, l'utilizzo del *dossier sanitario,* costituito presso un organismo sanitario in qualità di unico titolare del trattamento, attraverso il quale sono rese accessibili informazioni relative ad eventi clinici presenti e trascorsi, volte a documentare la storia clinica di un individuo, l'Autorità Garante ha effettuato diversi accertamenti ispettivi presso aziende sanitarie pubbliche[1], nell'ambito dei quali sono stati accertati, tra le altre criticità, molti casi di accessi abusivi ai dossier sanitari da parte di soggetti non autorizzati, resi possibili oltre che **dall'inadeguatezza delle misure di sicurezza organizzative e tecniche adottate, anche dalla carente sensibilizzazione e formazione del personale in materia di protezione dei dati personali.**

A seguito delle criticità riscontrate durante i predetti accertamenti e considerato il sempre maggiore utilizzo di strumenti di condivisione informatica di dati e documenti nell'ambito delle attività cliniche delle aziende sanitarie pubbliche e private**, l'Autorità Garante ha ritenuto**

opportuno adottare, con il provvedimento n. 331 del 04.06.2015, delle nuove linee guida in materia di dossier sanitario, al fine di fornire un quadro di riferimento unitario per conformare i trattamenti di dati personali, effettuati tramite i dossier sanitari, ai principi e agli obblighi previsti dalla normativa in materia di protezione dei dati personali, con particolare riferimento **all'informativa, al consenso, ai diritti degli interessati e alle misure di sicurezza organizzative e tecniche**.

Un recente caso di data breach, avvenuto tramite il dossier sanitario, sanzionato dall'Autorità Garante

Nel ricordare che anche successivamente all'adozione delle nuove linee guida in materia di dossier sanitario, l'Autorità Garante ha dovuto intervenire, a seguito di specifiche segnalazioni, presso alcune aziende sanitarie con propri provvedimenti prescrittivi e sanzionatori[2], nel seguito si ritiene opportuno **analizzare il provvedimento del 23. 01. 2020 (doc. web n. 9269629) con il quale è stata sanzionata un'importante azienda sanitaria pubblica per data breach** causati da alcuni accessi a dossier sanitari, non giustificati da necessità di cura dei relativi pazienti.

Nelle premesse del provvedimento viene fatto riferimento al fatto che l'Azienda sanitaria, dopo aver riscontrato che **in tre diversi casi si era verificato un accesso improprio ad alcuni dossier sanitari di pazienti**, che erano al tempo stesso anche dipendenti, ha proceduto, ai sensi dell'art. 33 del GDPR, ad inoltrare la notifica della violazione di dati personali al Garante, dichiarando che gli accessi erano stati effettuati rispettivamente "*con le credenziali di un medico che, durante il turno notturno, ha lasciato incustodita e accessibile la postazione pc in uso, consentendo ad altri di accedere ai dati sanitari di sei pazienti/dipendenti*", "*da un tecnico sanitario di radiologia, al fine di vedere come funzionava l'applicazione*" e per "*per mera curiosità*".

Nelle notifiche all'Autorità Garante, l'Azienda sanitaria dopo aver precisato che aveva 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 gli specializzandi), specifiche indicazioni in merito ai presupposti di liceità degli accessi al dossier sanitario aziendale, ha confermato 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", informando altresì di aver **avviato un procedimento disciplinare nei confronti dei dipendenti responsabili dei predetti accessi non autorizzati ai dossier sanitari**.

Conclusa l'attività istruttoria e tenuto conto delle memorie difensive presentate dall'Azienda sanitaria, il Garante, pur considerando che gli accessi impropri ai dossier sanitari sono da ascriversi a una "condotta infedele" di alcuni medici e tecnici sanitari di radiologia, ha ritenuto comunque illecito il trattamento, in quanto effettuato in violazione dell'art. 5.1.f del GDPR, decidendo:

- di ingiungere, quale misura correttiva, di completare entro 90 giorni l'implementazione

delle misure descritte nelle memorie difensive, volte a migliorare le procedure di accesso ai dossier sanitari aziendali da parte del personale a ciò autorizzato.
- di ordinare il pagamento della somma di euro 30.000 a titolo di sanzione amministrativa pecuniaria;
- di disporre, ai sensi dell'art. 166, comma 7, del D. Lgs. 196/03, la pubblicazione per intero sul sito web del Garante il provvedimento correttivo e sanzionatorio

Conclusioni

Il caso di data breach sopra analizzato, dimostra quanto sia indispensabile per le aziende sanitarie che intendono utilizzare strumenti di sanità digitale, qual è appunto il dossier sanitario, non solo **effettuare prioritariamente un'approfondita analisi dei rischi** che tale utilizzo può comportare per i diritti e le libertà fondamentali degli interessati e, conseguentemente, **adottare le necessarie misure organizzative e tecniche ritenute adeguate per garantire un livello di sicurezza proporzionato ai rischi**, ma anche dotarsi di una procedura che consenta di testare, verificare e valutare costantemente l'efficacia di tali misure.

Un ulteriore insegnamento che si deve trarre dal caso di data breach appena analizzato, riguarda la **necessità che il processo di digitalizzazione nelle aziende sanitarie venga accompagnato da una costante ed adeguata attività di sensibilizzazione e di formazione del management e di tutti gli operatori sanitari,** sui principi e sugli obblighi di compliance previsti dalla vigente normativa europea e nazionale in materia di protezione dei dati personali.

In conclusione, ciò che emerge dall'analisi del provvedimento del Garante è che **gli accorgimenti e le cautele contenute nelle linee guida in materia di dossier sanitario vanno implementate alla luce delle novità introdotte dal GDPR**, con particolare riferimento al principio di *accountability* e a quello della *privacy by design e by default*. Solo nel rispetto di tali principi, infatti, è possibile che il pur auspicabile utilizzo delle soluzioni di sanità elettronica da parte delle aziende sanitarie, venga effettuato nel rispetto dei diritti e delle libertà fondamentali dei pazienti.

[1] Si vedano in particolare i seguenti provvedimenti: "Dossier sanitario e trattamento dei dati personali dei pazienti" del 10.01.2013 (doc. web n. 2284708); "Trattamento di dati tramite il dossier sanitario aziendale" del 03.07.2014 (doc. web n. 3325808); "Dossier sanitario elettronico e privacy dei pazienti" del 23.10.2014 (doc. web n. 3570631); "Illiceità nel trattamento di dati personali e sensibili presso una struttura ospedaliera" del 18.12.2014 (doc. web n. 3725976);

[2] Si vedano, ad esempio, i seguenti provvedimenti: "Ordinanza ingiunzione nei confronti di Azienda Unità Sanitaria Locale di Piacenza" del 06.06.2018 (doc. web 9023253); "Ordinanza ingiunzione nei confronti di Azienda Sanitaria Locale di Alessandria" del 31.01.2019 (doc. web 9099205)