Dossier sanitario: le violazioni privacy più comuni nelle strutture

Il dossier sanitario è uno strumento chiave per la digitalizzazione della sanità, ma l'applicazione pratica solleva criticità legate al consenso, alla trasparenza e alla sicurezza dei dati, come dimostrano due recenti sanzioni del Garante privacy

(Fonte: **https://www.agendadigitale.eu/** 1° ottobre 2025)

Il Dossier Sanitario continua a far discutere. Da una parte rappresenta infatti uno strumento di importanza strategica nel percorso di digitalizzazione della sanità, migliorando la continuità e la qualità del processo di cura attraverso la raccolta organica della storia clinica del paziente; dall'altra la sua implementazione pratica si scontra con notevoli complessità e difficoltà, specie sotto il profilo di protezione dei dati.

È innegabile, infatti, che ogni volta che c'è un controllo, c'è sempre qualche profilo che è **non compliant con il GDPR** e/o con le Linee Guida.

È il caso di due recenti provvedimenti sanzionatori dell'Autorità Garante — uno contro l'Azienda Ospedaliero-Universitaria Careggi e l'altro contro la Casa di Cura Città di Roma — che gettano luce sulle criticità più comuni e profonde (presenti, devo dire, in numerose altre strutture che hanno adottato il Dossier).

L'analisi di questi casi offre quindi la possibilità **di valutare quali sono gli approcci non corretti** e, forse, anche di ragionare su possibili aperture interpretative.

Indice degli argomenti

Le violazioni riscontrate nel caso della Azienda Ospedaliero-Universitaria Careggi

In data 4 agosto è stato pubblicato sul sito del Garante Privacy il provvedimento contro l'Azienda Ospedaliero-Universitaria Careggi [doc. web n. 10166336], emblematico per la vastità delle problematiche riscontrate.

Vediamo le violazioni riscontrate.

Il consenso mancante e la trasparenza violata

La violazione più grave riscontrata è stata la totale assenza di un consenso specifico per la costituzione del dossier. L'Azienda si basava su un generico **consenso orale per finalità di cura**, e non era mai stato chiesto un consenso specifico per la costituzione del Dossier.

Di conseguenza, i pazienti non erano minimamente a conoscenza che la loro storia clinica venisse aggregata e resa accessibile trasversalmente all'interno della struttura.

Questa prassi ha comportato una palese violazione dei principi di **liceità e trasparenza** (art. 5, par. 1, lett. a) e art. 9 del GDPR), poiché il trattamento avveniva all'insaputa degli interessati, privandoli di ogni forma di controllo sui propri dati sanitari.

Accessi indiscriminati e privacy by design assente

La configurazione del sistema informativo permetteva al personale medico di accedere allo storico dei pazienti anche per episodi clinici avvenuti in **unità operative diverse** da quelle di propria competenza. Nello specifico, un medico poteva visualizzare la **lettera al curante o la relazione di degenza** di un paziente curato in un altro reparto.

Sebbene il sistema richiedesse al medico di dichiarare di aver ottenuto un "consenso verbale" dal paziente per tale accesso, questa misura si è rivelata **puramente fittizia**, dato che il paziente non era informato dell'esistenza stessa del dossier.

Questa carenza strutturale ha violato il principio di minimizzazione che limita l'accesso al solo personale sanitario effettivamente coinvolto nel processo di cura. L'assenza di filtri e barriere tecniche adeguate ha dimostrato una completa negligenza nell'applicazione del principio di **protezione dei dati fin dalla progettazione** (art. 25 GDPR), che impone al titolare di integrare le garanzie necessarie sin dal momento della progettazione dei sistemi di trattamento.

Diritti negati e controlli inesistenti

Le violazioni si estendevano anche alla negazione dei diritti fondamentali del paziente:

- **Diritto all'oscuramento:** I pazienti non solo non erano informati di questa facoltà, ma il sistema permetteva unicamente l'oscuramento dell'intera cartella sanitaria (ad eccezione della relazione di degenza), non del singolo evento clinico, rendendo di fatto il diritto inapplicabile.
- **Diritto di visione degli accessi:** Gli interessati non erano informati della possibilità di verificare chi avesse consultato il loro dossier.
- **Misure di sicurezza:** Era del tutto assente un sistema di **alert automatici** per il rilevamento di accessi anomali, una misura tecnica essenziale per garantire l'integrità e la riservatezza dei dati (art. 5, par. 1, lett. f) e art. 32 GDPR).

È significativo notare che l'Azienda ha avviato l'implementazione delle misure correttive necessarie, come l'introduzione di un'informativa adeguata e di un sistema di raccolta del

consenso tramite **codice OTP**, solo a seguito dell'ispezione del Garante, un fattore che ha pesato nella determinazione della sanzione.
La violazione, protrattasi per un lungo arco temporale (dal 2011 al 2025), ha coinvolto un numero altissimo di pazienti (**212.000 pazienti)** portando quindi all'irrogazione di una sanzione di **80.000 euro**.

Il caso della Casa di cura Città di Roma
Il provvedimento Garante Privacy 11 settembre 2025 [doc. web n. 10169116] contro la Casa di Cura Città di Roma dimostra che le medesime criticità non sono un'esclusiva delle grandi strutture pubbliche, ma possono manifestarsi con dinamiche simili anche in contesti privati di dimensioni più contenute.
Questo provvedimento fa emergere violazioni più sottili ma ugualmente gravi, legate a una configurazione del sistema informativo e a prassi operative non conformi ai principi fondamentali di protezione dei dati.

Un consenso viziato e l'obbligo di responsabilizzazione
A differenza del caso Careggi, la Casa di Cura acquisiva un consenso specifico per il dossier. Tuttavia, tale consenso era viziato alla radice: la firma per l'attivazione del dossier comportava **automaticamente l'espressione del "consenso al pregresso"**, ovvero l'inclusione di tutti i dati sanitari precedenti. Le Linee Guida del Garante, invece, richiedono un consenso specifico e separato anche per questa operazione.
Inoltre, la struttura non è stata in grado di comprovare le modalità di diniego del consenso per **2.973 pazienti**, violando palesemente il **principio di accountability** (art. 5, par. 2 GDPR), che impone al titolare non solo di rispettare le norme, ma anche di essere in grado di dimostrare tale rispetto.

La violazione dei principi di finalità e minimizzazione
I profili di autorizzazione si sono rivelati gravemente inadeguati e non selettivi:

- Un **medico** (ad esempio un ortopedico) poteva accedere alla documentazione sanitaria di *tutti* i pazienti ricoverati e dimessi in *tutti* i reparti della struttura, anche in assenza di qualsiasi coinvolgimento nel loro percorso di cura.
- Il **personale infermieristico e amministrativo** aveva accesso a un volume di informazioni sanitarie eccessivo e non necessario per le proprie mansioni, come diagnosi d'ingresso e Schede di Dimissione Ospedaliera (SDO) complete.

Questa configurazione trattava l'intero database clinico come un'entità monolitica, contraddicendo direttamente il requisito del GDPR di un controllo degli accessi granulare e orientato alla finalità, che è l'essenza pratica del principio di minimizzazione in un ambiente sanitario complesso.

Si è determinata così una chiara violazione dei **principi di limitazione della finalità e di minimizzazione dei dati** (art. 5, par. 1, lett. b) e c) GDPR).

Carenze tecniche e tracciabilità incompleta

La criticità tecnica più grave riscontrata era l'incapacità del sistema di **registrare le operazioni di sola "consultazione"** del dossier. Il software tracciava solo le operazioni di inserimento, modifica e cancellazione, ma non chi semplicemente visualizzava i dati.

Questa lacuna aveva un impatto importante sulla trasparenza e sulla sicurezza: rendeva infatti materialmente impossibile per la Casa di Cura rispondere a un'eventuale richiesta del paziente di visionare gli accessi al proprio dossier, svuotando di fatto un diritto fondamentale del paziente.

Anche in questo caso, le misure correttive, come l'attivazione di uno **specifico modulo software per la registrazione dei log di consultazione**, sono state implementate solo dopo l'intervento del Garante.

La sanzione, di "soli" **12.000 euro**, ha tenuto conto dello stato di liquidazione della società.

Ripensare la base giuridica del consenso

L'analisi dei casi dell'Azienda Careggi e della Casa di Cura Città di Roma, seppur diversi per scala e contesto, rivelano **un quadro coerente di difficoltà sistemiche nell'applicazione della normativa sul Dossier Sanitario**: difficoltà e violazioni che, peraltro, sono le stessi che si ripetono anche in altri passati provvedimenti del Garante.

Allora occorre domandarsi se i problemi (che si riscontrano di frequente anche in sede di consulenza) siano più di natura informatica o organizzativa o giuridica. Oppure – come credo – i tre elementi insieme.

Cogliamo allora l'occasione per alcune considerazioni.

Partiamo dalla base giuridica del consenso, che resta un punto debole, in quanto spesso non raccolto o raccolto con modalità non conformi o viziate.

Tale base giuridica era stata prevista come obbligatoria dalle Linee Guida del 2015; provvedimento però assunto prima del GDPR, in vigenza di una architettura giuridica completamente diversa ed altresì applicabili, secondo l'art. 20 del D.Lgs 101/'98, solo "ove compatibili".

Alla luce di quanto sopra ci possiamo quindi domandare se oggi, in vigenza dell'art. 9 lett. h) GDPR e con la cresce digitalizzazione della sanità, il Dossier sanitario non possa essere considerato come parte integrante del trattamento "necessario" per finalità di diagnosi e cura (lett. h), data la sua funzione ormai essenziale per garantire la continuità e la sicurezza delle cure nell'era digitale.

Privacy by design come unica soluzione

Questo spostamento della base giuridica snellirebbe le procedure di attivazione, riconoscendo il dossier come parte intrinseca e non più opzionale del percorso di cura moderno.

Questo peraltro non farebbe venir meno le altre garanzie e quindi **non indebolirebbe affatto la protezione del paziente**.

La limitazione granulare degli accessi, le misure tecniche di controllo e tracciabilità (come i sistemi di alert e la registrazione completa dei log di consultazione) i diritti dell'interessato come l'oscuramento selettivo, sono tutti profili previsti nelle Linee Guida che oggi devono essere considerati pienamente validi e, anzi, ancora più cogenti in quanto espressione diretta dei principi fondamentali del GDPR (art. 5).

Quindi, se riteniamo che la maggior digitalizzazione della sanità sia una frontiera per innalzare la qualità delle cure e se altresì reputiamo che i dati digitali possano essere uno strumento di crescita per le cure, per l'organizzazione e per la ricerca, dobbiamo abbracciare **una logica di protezione "fin dalla progettazione e per impostazione predefinita" (*privacy by design & by default*).**

Non si possono essere più scuse giuridiche, organizzative o informatiche.