- Academy FPA -

#forumpa2016

Privacy in ambito sanitario

Avvocato Cristina Daga

Indice

- Brevi cenni sul nuovo Regolamento UE e impatto sul settore sanitario
- Dossier sanitario
- Brevi cenni sui referti on line
- Brevi cenni sul fascicolo sanitario elettronico

Regolamento UE e impatto sul settore sanitario

Regolamento UE e impatto sul settore sanitario

- In data 14 aprile 2016 è stato approvato dal Parlamento europeo il Regolamento in materia di protezione dei dati personali (pubblicato in GUE il 04 maggio 2016, entrato in vigore il 24 maggio 2016).

- Il testo di legge, oggi a disposizione, è quello approvato l'8 aprile 2016 dal Consiglio Europeo.

- Il Regolamento non contiene specifiche disposizioni in materia di privacy e sicurezza nel settore sanitario;

Regolamento UE e impatto sul settore sanitario

- Preambolo Regolamento:

(Considerando 35)

- nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso, fra cui:
  - le **informazioni** raccolte nel corso della sua **registrazione** al fine di **ricevere servizi** di **assistenza sanitaria;**
  - un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco **a fini sanitari**;
  - le **informazioni** risultanti da **esami** e **controlli** effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici;
  - qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o l'effettivo stato fisiologico o biomedico dell'interessato.

Regolamento UE e impatto sul settore sanitario

- Preambolo Regolamento:

(Considerando 53)

- Le categorie particolari di dati personali che **necessitano di una maggiore protezione** possono essere trattate soltanto per finalità connesse alla salute, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria (…);

Regolamento UE e impatto sul settore sanitario

- Preambolo Regolamento:

(Considerando 53)

- Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche;

- gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di:
  - dati genetici;
  - dati biometrici;
  - dati relativi alla salute.

Decreto legislativo 196/2003

Principi generali sul trattamento dei dati personali in ambito sanitario

- <u>Alcuni principi applicabili al trattamento di dati sensibili per i soggetti pubblici</u>
  - L'art. **22 D. Lgs 196/2003** stabilisce che:

1. I soggetti pubblici possono trattare solo dati sensibili indispensabili per svolgere attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali di diversa natura (art. 22, 3 comma).

1. i dati sensibili sono raccolti, di regola, presso l'interessato (art. 22, 4 comma).

1. **I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo** (art. 22, 7 comma).

1. I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 22, 8 comma).

Principi generali sul trattamento dei dati personali in ambito sanitario

- <u>Alcuni principi applicabili al trattamento di dati sensibili per i soggetti privati</u>
  - L'art. **23** e **26 D. Lgs 196/2003** stabilisce che:

1. Il trattamento dei dati sensibili è ammesso solo con il consenso scritto dell'interessato (art. 23, 1 comma).

2. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili (art. 23, 4 comma).

3. I dati sensibili possono essere oggetto di trattamento solo **con il consenso scritto dell'interessato e previa autorizzazione del Garante,** nell'osservanza dei presupposti e dei limiti stabiliti dal codice, nonché dalla legge e dai regolamenti (art. 26, 1 comma).

4. I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 26, 5 comma).

Principi generali sul trattamento dei dati personali in ambito sanitario

- **Nell'ambito sanitario, accade che i dati sensibili del paziente siano raccolti anche presso terzi legittimati, come ad esempio**:
  - Coniuge o convivente;
  - Chi esercita la patria potestà;
  - Familiari
  - Altri soggetti

- **I soggetti terzi legittimati sono individuati:**
  - dal medico e/o dalla struttura sanitaria nei casi in cui il paziente sia incapace naturale;
  - dal paziente (al momento del consenso) nei casi in cui sia capace d'agire;

Principi generali sul trattamento dei dati personali in ambito sanitario

- L'art. **77**, del **D. Lgs 196/2003** disciplina le **modalità semplificate per la consegna dell'informativa, per la raccolta del consenso** e per il trattamento dei dati personali. Le modalità semplificate sono applicabili:
    - dagli organismi sanitari pubblici;
    - dagli altri organismi privati e dagli esercenti le professioni sanitarie;
    - dagli altri soggetti pubblici.

- Ai sensi dell'**art. 78** del **D. Lgs 196/2003** il medico di medicina generale o il pediatra di libera scelta informa l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da **rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1** .

Principi generali sul trattamento dei dati personali in ambito sanitario

- L'informativa può essere fornita per il **complessivo trattamento** dei dati personali necessario per attività di **prevenzione, diagnosi, cura e riabilitazione,** svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse (modalità semplificate).

- **L'informativa evidenzia analiticamente eventuali trattamenti di dati personali, anche in caso di trattamenti effettuati:**
  - per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti;
  - nell'ambito della teleassistenza o telemedicina;
  - per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Principi generali sul trattamento dei dati personali in ambito sanitario

- L'art. **79**, **D. Lgs 196/2003** disciplina l'informativa da parte degli organismi sanitari.

1 Gli organismi sanitari **pubblici e privati** possono avvalersi delle modalità semplificate relative all'informativa e al consenso **in riferimento ad una pluralità di prestazioni** erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati.

1 Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta informativa e il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

1 Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità semplificate possono essere utilizzate per più trattamenti di dati.

Principi generali sul trattamento dei dati personali in ambito sanitario

- L’art. **81, D. Lgs 196/2003** disciplina il consenso da parte degli interessati.

  - Il consenso al trattamento dei dati idonei a rivelare lo stato di salute **può essere manifestato con un'unica dichiarazione, anche oralmente.** In **tal caso il consenso è documentato,** anziché con atto scritto dell'interessato, **con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico,** riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato.

Principi generali sul trattamento dei dati personali in ambito sanitario

- L'art. **82, co. II** del **D. Lgs 196/2003** disciplina i principi generali in tema di trattamento dei dati personali in ambito sanitario. L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di:
    - **impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato,** quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;
    - **rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.**

- L'i**nformativa** e il **consenso** al trattamento dei dati personali possono **intervenire senza ritardo, successivamente** alla **prestazione**, anche in caso di **prestazione medica** che può essere **pregiudicata** dall'**acquisizione preventiva del consenso**, in termini di tempestività o efficacia.

- **Dopo** il **raggiungimento** della **maggiore età** l'informativa è fornita all'interessato anche ai fini della acquisizione di una **nuova manifestazione del consenso** quando questo è necessario.

Notificazione

- Art. **37 D.lgs 196/2003** Notificazione

  Il titolare deve notificare al Garante il trattamento di dati personali cui intende procedere, se il trattamento riguarda:

  a) dati **genetici**, **biometrici** o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

  b) dati idonei a rivelare lo **stato di salute** e la vita sessuale, trattati a fini di procreazione assistita, **prestazione di servizi sanitari** per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria (...).

Notificazione

- Art. **37 D. lgs 196/2003** - Chiarimenti sui trattamenti da notificare al Garante - 23 aprile 2004

  - Dati sulla salute o sulla vita sessuale utilizzati per prestare servizi sanitari per via telematica (art. 37, comma 1, lett. B).

  - **É tenuto alla notificazione chi eroga servizi sanitari per via telematica relativi ad una banca di dati o alla fornitura di beni.**

  - Non devono essere quindi notificati i trattamenti di dati sanitari - e/o sulla vita sessuale- effettuati nell'ambito di *servizi di assistenza o consultazione sanitaria per via telefonica*, come i servizi telefonici gestiti in ambito assicurativo e che consentono il consulto di esercenti professioni sanitarie.

Obblighi di sicurezza nel trattamento dei dati personali in ambito sanitario

Misure idonee di sicurezza

Le misure idonee di sicurezza sono previste dall'art 31 D.lgs 196/2003:

- I titolari del trattamento, al fine di ridurre al minimo i rischi di:
  - distruzione o perdita, anche accidentale, dei dati,
  - accesso non autorizzato ai dati,
  - trattamento dei dati non consentito o non conforme alle finalità della raccolta,

DEVONO ADOTTARE MISURE DI SICUREZZA PREVENTIVE

ED IDONEE A PROTEGGERE I DATI.

- **L'adozione di tali misure è correlata:**
  - alla natura dei dati
  - alle specifiche caratteristiche del trattamento
  - al progresso tecnico

Misure minime di sicurezza (1/3)

- Le misure minime per la sicurezza dei dati, anche di natura sensibile, previste dagli articoli 33 e ss. e nell'Allegato B del D. Lgs 196/2003 si distinguono in:

- Misure minime di sicurezza per il trattamento dei dati <u>con strumenti elettronici</u>

  a) Sistemi di autenticazione;

  b) Sistemi di autorizzazione;

  c) Altre misure di sicurezza;

  d) Misure di sicurezza per il trattamento dei dati sensibili e giudiziari

❑ Misure minime di sicurezza per il trattamento dei dati **<u>senza ausilio di strumenti elettronici</u>**

Misure minime di sicurezza (2/3)

- Trattamento dei dati con strumenti elettronici (Trattamento di dati sensibili)

a) I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (punto 20)

b) Sono impartite istruzioni organizzative e tecniche per **la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti** (punto 21).

a) I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (punto 22).

b) Sono adottate **idonee misure per garantire il ripristino dell'accesso ai dati** in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (punto 23).

Misure minime di sicurezza (3/3)

- Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati tenuti con l'ausilio di strumenti elettronici:

  d) **Con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che**, considerato il numero e la natura dei dati trattati, **li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (art. 22, 6 comma).**

  e) Anche al **fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati (art. 22, 7 comma).**

- **I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato (punto 24).**

Dossier Sanitario Elettronico

Fonti normative

- Linee Guida in tema di Fascicolo sanitario elettronico e di Dossier Sanitario del Garante per la protezione dei dati personali - 16 luglio 2009

- Linee Guida in materia di Dossier sanitario del Garante per la protezione dei dati personali– 4 Giugno 2015 varate al fine di definire un quadro di riferimento unitario per il corretto trattamento dei dati raccolti **nei dossier, già istituiti o che si intendono istituire**, da parte di **strutture sanitarie pubbliche e private**.

Le Linee Guida in materia di dossier sanitario. Definizione

- Il dossier sanitario elettronico viene definito nelle Linee guida come «lo strumento costituito presso un'unica struttura sanitaria (ospedale, azienda sanitaria, casa di cura) che raccoglie informazioni sulla salute di un paziente al fine di documentarne la storia clinica presso quella singola struttura e offrirgli un migliore processo di cura».

- Il dossier sanitario, dunque, contiene dati relativi agli eventi clinici occorsi all'interessato esclusivamente presso un'unica struttura sanitaria.

- Si differenzia dal Fascicolo sanitario elettronico (FSE) per la circostanza che i documenti e le informazioni sanitarie accessibili tramite tale strumento sono state generate da un solo titolare del trattamento e non da più strutture sanitarie in qualità di autonomi titolari, come avviene proprio per il FSE.

Caratteristiche del trattamento effettuato tramite il dossier

- Il dossier sanitario, essendo finalizzato a documentare parte della storia clinica dell'interessato attraverso la **realizzazione di un sistema integrato delle informazioni sul suo stato di salute** **accessibile da parte del personale sanitario che lo ha in cura**, costituisce uno trattamento di dati personali specifico ed ulteriore rispetto a:

  - **quello relativo alla compilazione e tenuta della cartella clinica**, intesa come lo strumento informativo individuale finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente e **ad un singolo episodio di ricovero**.

  - quello effettuato dal professionista sanitario con le **informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso**:

    - **in assenza del dossier sanitario**, infatti, il professionista avrebbe accesso alle sole informazioni fornite in quel momento dal paziente e a quelle elaborate in relazione all'evento clinico per il quale lo stesso ha richiesto una prestazione sanitaria;

    - **attraverso il dossier sanitario**, invece, il professionista pone in essere un ulteriore trattamento di dati sanitari mediante la consultazione delle informazioni elaborate in occasione di altri eventi clinici occorsi, anche da altri professionisti;

Principali rischi connessi all'utilizzo di dossier sanitari (1/3)

- Dall'esame di numerosi dossier sanitari, il Garante ha potuto riscontrare la tendenza, da parte delle strutture sanitarie, a sviluppare tali strumenti in modo non strutturale e organizzato, senza tener conto del fatto che si andava predisponendo un sistema informativo in grado di gestire potenzialmente l'intera storia clinica di un individuo.

- I principali rischi connessi allo sviluppo estemporaneo di dossier riscontrati dall'Autorità Garante sono i seguenti:
  - la **mancanza di certezza sull'autenticità delle informazioni**;
  - la **possibilità che le informazioni siano accessibili e modificabili da parte di soggetti non legittimati o siano persino diffuse**;
  - la **non disponibilità delle informazioni**;
  - Il **furto o smarrimento** parziale o integrale **dei supporti di memorizzazione o dei sistemi di elaborazione** portatili o fissi.

Principali rischi connessi all'utilizzo di dossier sanitari (2/3)

- I dossier sanitari, anche al fine di costituire un effettivo strumento di ausilio nei processi di diagnosi e cura dei pazienti, devono invece essere realizzati con modalità tali da garantire:
  - **certezza dell'origine dei dati;**
  - **certezza della correttezza dei dati;**
  - **accessibilità degli stessi solo da parte di soggetti legittimati**.

Principali rischi connessi all'utilizzo di dossier sanitari (3/3)

- A fronte dei rischi e della complessità della materia, attraverso le Linee guida, l'Autorità Garante ha delineato un quadro di riferimento per i titolari dei trattamenti di dati che impone loro di conformare tali trattamenti ai principi di legittimità stabiliti dal Codice della Privacy, nel rispetto di elevati standard di sicurezza.

- Più dettagliatamente, il Garante ha imposto ai titolari, in considerazione della particolare delicatezza dei dati personali trattati mediante il dossier sanitario, l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).

Le principali indicazioni a tutela dei pazienti

- In ossequio ai principi sanciti dal Codice della Privacy, le Linee guida, relativamente al trattamento ed in particolare all'informativa da fornire all'interessato, stabiliscono che:
  - Ai pazienti deve essere consentito di **scegliere, in piena libertà, se far costituire o meno il dossier sanitario** (*trattamento facoltativo*).
  - Per consentire al paziente di scegliere in maniera libera e consapevole, **la struttura sanitaria dovrà informarlo in modo chiaro**, indicando in particolare:
    - **chi avrà accesso ai suoi dati**;
    - **che tipo di operazioni potrà compiere**.

Le principali indicazioni a tutela dei pazienti. L'informativa (1/5)

- 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 ed in particolare i seguenti contenuti:

  - deve contenere la **descrizione del dossier sanitario**, deve cioè 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;

  - deve informare l'interessato che **l'eventuale mancato consenso al trattamento dei dati personali mediante il dossier sanitario non incide sulla possibilità di accedere alle cure mediche** richieste;

  - deve rendere nota all'interessato anche la circostanza che, qualora acconsenta al trattamento dei suoi dati personali mediante il dossier sanitario, questo potrà essere consultato, nel rispetto dell'Autorizzazione generale del Garante, anche qualora ciò sia **ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività** (art. 76 del Codice e Autorizzazione generale del Garante n. 2/2014 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale dell'11 dicembre 2014).

  - deve informare l'interessato in merito **ai soggetti o alle categorie di soggetti ai quali possono essere comunicati i dati personali trattati mediante il dossier o che possono venirne a conoscenza in qualità di responsabili o incaricati** e che, in quanto dati idonei a rivelare lo stato di salute, gli stessi **non possono essere oggetto di diffusione**;

Le principali indicazioni a tutela dei pazienti. L'informativa (3/5)

- deve specificare l'eventualità che il dossier sanitario sia **consultabile anche da parte dei professionisti che agiscono in libera professione** intramuraria;
- deve contenere una **breve descrizione delle misure che sono state adottate** per la protezione dei dati da specifici rischi di accesso non autorizzato e di trattamento non consentito unitamente a quelle individuate per garantire l'esattezza, l'integrità e la continuità della fruibilità dei dati;
- deve indicare **le modalità attraverso le quali rivolgersi al titolare per esercitare i diritti di cui agli artt. 7 e ss. del Codice**, 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;
- deve contenere una **specifica menzione** 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 e di alcool; a donne che si sottopongono ad interruzione volontaria della gravidanza o che scelgono di partorire in anonimato ovvero a quelle rese in occasione di atti di violenza sessuale o di pedofilia o da parte dei consultori familiari).

Le principali indicazioni a tutela dei pazienti. L'informativa (5/5)

- L'informativa deve essere **fornita all'interessato prima dell'acquisizione del consenso** e, vista la particolare delicatezza dei dati personali trattati mediante il dossier sanitario, è necessario che la stessa sia **facilmente consultabile dall'interessato anche successivamente alla prestazioni del consenso.**

- In tal senso, l'Autorità ha apprezzato l'iniziativa di molte strutture sanitarie di pubblicare l'informativa sul proprio sito Internet o di affiggere la stessa nei locali di attesa delle prestazioni sanitarie.

- In caso di omessa o inidonea informativa all'interessato è prevista una sanzione amministrativa.

Le principali indicazioni a tutela dei pazienti. Il consenso (1/4)

- Le Linee guida, in ossequio ai principi sanciti dal Codice della Privacy, relativamente al trattamento ed in particolare al consenso dell'interessato stabiliscono che:

  - In **assenza del consenso** dell'interessato, il professionista che lo prende in cura avrà a disposizione solo le informazioni rese in quel momento dallo stesso interessato (ad es., raccolta dell'anamnesi e delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista.

  - Analogamente, in tale circostanza il **personale sanitario di reparto/ambulatorio** avrà accesso solo alle informazioni relative all'episodio per il quale l'interessato si è rivolto presso quella struttura e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio **(c.d. accesso agli applicativi verticali dipartimentali).**

Le principali indicazioni a tutela dei pazienti. Il consenso (2/4)

- Una volta **prestato il consenso** al trattamento dei dati personali mediante il dossier sanitario, quest'ultimo sarà **accessibile da parte di tutti gli operatori sanitari che, nel corso del tempo, lo prenderanno in cura, senza che l'interessato debba manifestare tale volontà ogni volta che accede per vari motivi alla struttura sanitaria**.

- Il consenso al dossier, **anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura**, deve essere **autonomo e specifico**.

- In caso di incapacità di agire dell'interessato deve essere acquisito il consenso di chi esercita la potestà legale su di esso. In caso di minori, raggiunta la maggiore età, deve essere acquisito -al primo contatto utile- nuovamente il consenso informato dell'interessato divenuto maggiorenne.

Le principali indicazioni a tutela dei pazienti. Il consenso (3/4)

- L'inserimento delle i**nformazioni relative ad eventi sanitari pregressi all'istituzione del dossier sanitario** deve, inoltre, fondarsi sul **consenso specifico ed informato dell'interessato,** potendo quest'ultimo anche scegliere che le informazioni sanitarie pregresse che lo riguardano non siano trattate mediante il dossier.

- In caso di **revoca del consenso** (**liberamente manifestabile in qualsiasi momento**), **il dossier sanitario non deve essere ulteriormente implementato**. Le informazioni sanitarie presenti devono restare disponibili al professionista o alla struttura interna al titolare che le ha redatte (ad es., informazioni relative a un ricovero utilizzabili solo dal reparto di degenza) e per eventuali conservazioni per obbligo di legge, **ma non devono essere più condivise con i professionisti degli altri reparti che prenderanno in seguito in cura l'interessato**.

Le principali indicazioni a tutela dei pazienti.
Il consenso (4/4)

- Il trattamento dei dati personali in violazione delle disposizioni sul consenso costituisce una fattispecie sanzionabile amministrativamente, rilevante anche in sede penale. Il trattamento dei dati personali effettuato mediante il dossier sanitario in assenza del consenso informato dell'interessato, invero, non è lecito (trattamento illecito di dati, art. 167 co 2 Codice Privacy). I dati personali in tal modo trattati non possono essere utilizzati da parte del titolare.

Le principali prescrizioni per i titolari del trattamento (1/2)

- La struttura sanitaria, in qualità di titolare del trattamento dati mediante dossier sanitario deve:
  - individuare le **modalità attraverso le quali i soggetti autorizzati ad accedere al dossier sanitario possano verificare che sia stata resa l'informativa e acquisito il consenso dell'interessato** al trattamento dei suoi dati personali mediante il dossier sanitario;
  - garantire al paziente **l'esercizio dei diritti riconosciuti dal Codice privacy** (accesso ai dati, integrazione, rettifica, etc.) e la possibilità di **conoscere il reparto, la data e l'orario in cui è avvenuta la consultazione del suo dossier**;
  - garantire al paziente la possibilità di «**oscurare» alcuni dati o documenti sanitari** che non intende far confluire nel dossier

Le principali prescrizioni per i titolari del trattamento (1/2)

- nell'indicare i soggetti che in qualità di responsabili o incaricati del trattamento possono accedere al dossier sanitario, deve **illustrare anche l'adozione degli specifici criteri di profilazione degli utenti adottati**.

- Tali criteri di profilazione devono essere improntati al principio generale secondo cui **l'accesso al dossier sanitario è consentito ai soli professionisti sanitari che a vario titolo** (ad es., erogazione della prestazione, richiesta di consulenza) **e nel tempo hanno in cura il paziente**.

Diritti dell'interessato – art.7 D.lgs 196/2003

- L'interessato ha diritto di:
  - ottenere la **conferma circa l'esistenza o meno di dati che lo riguardano, la loro comunicazione in forma intelligibile, l'indicazione della loro origine, delle finalità e modalità del trattamento** (art. 7 del Codice);
  - poter ottenere **l'indicazione della logica applicata a tale trattamento** ovvero l'indicazione dei criteri utilizzati nell'elaborazione elettronica dei dati;
  - di avere l'indicazione del **titolare del trattamento, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati**;
  - **richiedere di integrare, rettificare, aggiornare i dati trattati mediante il dossier sanitario**;

Diritti dell'interessato - Oscuramento

- **Oscurare taluni dati o documenti sanitari** consultabili tramite tale strumento.

- 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»).**

    - Nel caso in cui l'interessato richieda l'oscuramento delle informazioni e/o dei documenti, 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

Diritti dell'interessato – Accessi eseguiti

- avanzare le richieste volte 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 (dell'esercizio, da parte dell'interessato, di tale diritto devono essere opportunamente informati anche i soggetti autorizzati ad accedere al dossier sanitario).

Accesso al dossier – Finalità di cura (1/3)

- Al fine di scongiurare il rischio di un accesso a tali informazioni da parte di soggetti non autorizzati o di comunicazione a terzi delle stesse da parte di soggetti a ciò abilitati, **le Linee guida impongono al titolare di porre una particolare attenzione nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati.**

- L'accesso al dossier deve essere limitato, quindi, al solo personale sanitario che interviene nel tempo nel processo di cura del paziente. Ciò significa che deve essere consentito l'accesso a tutto il personale **che a vario titolo interviene nel processo di cura**, come ad esempio quello operante nel reparto in cui è ricoverato il paziente, o che è stato coinvolto nella richiesta di una consulenza.

- Le Linee guida prescrivono al titolare di valutare, in relazione ai diversi profili di autenticazione al dossier, se sia indispensabile che siano in concreto accessibili tutti i dati presenti nello stesso o solo una parte di essi.

Accesso al dossier - Finalità di cura (2/3)

- Al fine di consentire che abbia accesso al dossier solo il personale sanitario coinvolto -a vario titolo e nel tempo - nel processo di cura del paziente, devono essere adottate modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria:

  - più specificatamente, il titolare del trattamento deve effettuare un monitoraggio delle i**potesi** in cui il relativo personale sanitario può avere necessità di consultare il dossier sanitario, per finalità di cura dell'interessato e, in base a tale ricognizione, individuare i diversi profili di autorizzazione all'accesso.

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

Accesso al dossier – Finalità amministrative (3/3)

- E’ stato infatti riscontrato che i dossier venivano utilizzati **anche per svolgere delle funzioni amministrative strettamente connesse con il percorso di cura del paziente** (prenotazione di esami clinici; richiesta di copia delle cartelle cliniche; indicazione a terzi legittimati della presenza in reparto di un degente; gestione dei posti letto, etc);

- in tali casi, il titolare deve prevedere delle **limitazioni alla «profondità di accesso» al dossier da parte del personale preposto a tali funzioni,** consentendo allo stesso di accedere ai soli dati indispensabili per svolgere i compiti ad essi demandati.

- Devono essere, pertanto, preferite soluzioni che **consentano un’organizzazione modulare dei *dossier*,** in modo tale da limitare l’accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al **modulo di dati**) indispensabili al raggiungimento dello scopo per il quale è stata consentita l’accessibilità al *dossier*.

Misure di Sicurezza. Sistemi di autenticazione e autorizzazione

- Considerata la particolare delicatezza del dossier il Garante ha prescritto l'adozione di elevate misure di sicurezza.

- In particolare, l'Autorità ha indicato al titolare del trattamento dei dati personali effettuato mediante il dossier sanitario le seguenti misure :

  - **SISTEMI DI AUTENTICAZIONE E DI AUTORIZZAZIONE**

    - Come già anticipato, il titolare del trattamento deve adottare **idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli nonché delle concrete esigenze di accesso ai dossier da parte del personale sanitario e amministrativo**, sia sulla base di una **specifica analisi del contesto organizzativo nel quale sono resi i servizi sanitari**, sia a seguito di un **monitoraggio delle casistiche per le quali il personale ha necessità di consultare i dossier sanitari**.

    - Tali sistemi devono garantire un **accesso selettivo al dossier sanitario fondato sul principio di indispensabilità del dato trattato**: il titolare del trattamento deve consentire l'accesso al dossier solo al personale sanitario coinvolto nel processo di cura e a quello amministrativo per le sole finalità strettamente correlate alla cura.

    - Il titolare deve inoltre individuare **procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati**.

Misure di Sicurezza. Tracciabilità degli accessi e delle operazioni (1/2)

- **TRACCIABILITÀ DEGLI ACCESSI E DELLE OPERAZIONI EFFETTUATE**

  - le strutture sanitarie devono **realizzare sistemi di controllo delle operazioni effettuate sul dossier sanitario**, mediante **procedure che prevedano la registrazione automatica in appositi file di log degli accessi e delle operazioni compiute** (ferma restando la disciplina in materia di controllo a distanza dell'attività dei lavoratori)

  - In particolare, **i file di log devono registrare per ogni operazione di accesso al dossier effettuata da un incaricato, almeno le seguenti informazioni**:

    - il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso;
    - la data e l'ora di esecuzione;
    - il codice della postazione di lavoro utilizzata;
    - l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

Misure di Sicurezza. Tracciabilità degli accessi e delle operazioni (2/2)

- In ragione della particolare delicatezza del trattamento dei dati personali effettuato mediante il dossier, è necessario che siano **tracciate anche le operazioni di semplice consultazione** (*inquiry*).

- Il titolare deve individuare un **congruo periodo di conservazione dei log** di tracciamento delle operazioni che risponda, da un lato, all'esigenza per gli interessati di venire a conoscenza dell'avvenuto accesso ai propri dati personali e delle motivazioni che lo hanno determinato e, dall'altro, alle esigenze medico legali della struttura sanitaria titolare del trattamento di dati personali (il Garante ha ritenuto congruo stabilire che i log delle operazioni siano conservati per un periodo non inferiore a **24 mesi dalla data di registrazione dell'operazione**).

Misure di Sicurezza. Sistemi di audit log (1/2)

- **SISTEMI DI AUDIT LOG**
  - 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 e, quindi, successivamente prefigurare l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento (ad es., relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).**

Misure di Sicurezza. Sistemi di audit log (2/2)

- L’attività di controllo deve essere **adeguatamente documentata** in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

- L’esito dell'attività di controllo **deve essere comunicato** alle persone e agli organi legittimati ad adottare decisioni e messo a disposizione del Garante, in caso di specifica richiesta.

Misure di Sicurezza. Separazione e cifratura dei dati

- **SEPARAZIONE E CIFRATURA DEI DATI**

  - Il titolare deve individuare **criteri per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali**.

  - Devono essere, inoltre, determinati i **criteri per la cifratura dei dati sensibili** (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database), **al fine di rendere gli stessi inintelligibili**.

Data breach. Comunicazioni al Garante

- Le peculiari caratteristiche del trattamento dei dati effettuato mediante il dossier sanitario, strettamente connesse alla delicatezza delle informazioni trattate, nonché all'esigenza di garantire l'esattezza, l'integrità e la disponibilità dei dati e la protezione da accessi non autorizzati e da trattamenti non consentiti, rendono necessario assoggettare il loro trattamento **all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati (*Data Breach*) o incidenti informatici (accessi abusivi, azione di malware…) che, pur non avendo un impatto diretto sui dati stessi, possano comunque esporli a rischi di violazione.**

- A questo fine, entro quarantotto ore dalla conoscenza del fatto, i titolari devono comunicare (secondo lo schema riportato nell'"Allegato B" alle Linee guida) all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

Data breach. Comunicazioni al Garante

- Tali comunicazioni devono essere redatte e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.dossier@pec.gpdp.it.

- La mancata comunicazione al Garante delle suddette violazioni o dei predetti incidenti informatici configura un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter, del Codice (la sanzione del pagamento di una somma da trentamila euro a centottantamila euro).

Data breach. Comunicazione all'interessato

- In ragione della particolare delicatezza del trattamento dei dati effettuato mediante il dossier sanitario, l'Autorità ritiene necessario che il titolare individui una procedura per comunicare senza ritardo all'interessato le operazioni di trattamento illecito effettuate dagli incaricati o da chiunque sui dati personali trattati mediante il relativo *dossier*.

- Tale tempestiva informazione, infatti, può consentire all'interessato di minimizzare i rischi connessi alla violazione della disciplina di protezione dei dati personali.

Data Protection Officer

- In sintonia con quanto espresso nel parere in materia di Fascicolo Sanitario Elettronico, il Garante auspica che i titolari del trattamento individuino al loro interno una figura di responsabile della protezione dei dati che svolga il ruolo di referente con il Garante (c.d. DPO - *Data Protection Officer)*, anche in relazione ai possibili casi di data breach.

Fare clic per inserire il contenuto