Privacy e sicurezza nella gestione dei dati clinici

Gabriele Faggioli
Adjunct Professor MIP-Politecnico di Milano
Presidente CLUSIT (Associazione Italiana per la Sicurezza Informatica)

23 ottobre 2015

- **La disciplina giuridica applicabile è contenuta:**
  - Art. 75 e ss. del d. lgs. 196/2003;
  - Altre Leggi nazionali **(come ad es. D.L. 179/2012, modificato dal D.L. 69/2013);**
  - Leggi regionali;
  - Provvedimenti e linee guida dell'Autorità Garante;

Le disposizioni contenute nelle normative richiamate garantiscono **l'assoluta riservatezza** e la **dignità** di tutte le persone che entrano in contatto con medici e strutture sanitarie per cure, prestazioni mediche, acquisto di medicine e operazioni amministrative (pagamenti e prenotazioni)

I dati trattati dai medici e dalle strutture sanitarie nell'esercizio dello loro attività sono di natura sensibile

- **Il Garante con Autorizzazione n. 2/2014 – *«Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale»*** individua anche altre misure per la sicurezza dei dati sensibili nel settore sanitario.

- **Il Garante con autorizzazione n. 8/2014 – *«Autorizzazione generale al trattamento dei dati genetici»*** indica anche le misure di sicurezza da adottare per la custodia e la sicurezza dei dati genetici e dei campioni biologici.

- Le misure per la sicurezza dei dati, anche di natura sensibile, previste dall'art. 31 del D. Lgs. 196/2003 sono volte a:

- I dati personali oggetto di trattamento **sono custoditi e controllati**, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo, mediante l'adozione di IDONEE e preventive misure di sicurezza, i rischi :**
  - **di distruzione o perdita, anche accidentale, dei dati stessi;**
  - **di accesso non autorizzato;**
  - **di trattamento non consentito o non conforme alle finalità della raccolta.**

•Il Provvedimento sulle strutture sanitarie del 2005 indica e ribadisce altri adempimenti da rispettare:

- **alla notificazione al Garante,** dovuta nei soli casi di cui all'art. 37 del Codice;
- **alla predisposizione dell'informativa da fornire agli interessati** (art. 13 del Codice);
- **all'acquisizione del consenso per i trattamenti di dati personali connessi all'erogazione delle prestazioni e dei servizi per svolgere attività di prevenzione, diagnosi, cura e riabilitazione** (artt. 22, 26 e 76 del Codice);
- per gli organismi sanitari pubblici, al rispetto delle disposizioni contenute nel regolamento per il trattamento dei dati sensibili per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione adottato ai sensi dell'art. 20 del Codice (cfr. Provv. del 30 giugno 2005);
- **al rispetto delle autorizzazioni generali rilasciate dal Garante ed, in particolare, dell'autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale** (artt. 26 e 76 del Codice);
- **alle misure di sicurezza** (artt. 31-36 del Codice e allegato B) al Codice).

- Fonti normative:
  - Linee Guida del Garante in materia di **Dossier Sanitario** del 04 giugno 2015.
  - Decreto Legge 18 ottobre 2012, n. 179 – ***«ulteriori misure per la crescita del paese».***
  - Linee Guida nazionali del Ministero della salute sul Fascicolo Sanitario Elettronico;
  - Linee Guida per la presentazione dei piani di progetto regionali per il FSE del 31 marzo 2014 Agenzia per l'Italia Digitale e dal Ministero della salute:
    - Il DPCM sul fascicolo sanitario elettronico firmato il 3 settembre 2015 dal ministro Lorenzin (in attesa di pubblicazione in Gazzetta ufficiale).
  - *"Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario"*(provv. del 16 luglio 2009 citato).

- *Altri provvedimenti importanti*

  - *La conservazione in forma digitale della cartella clinica (d.l. 9 febbraio 2012, n.5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35, art. 47-*bis*, comma 1-*bis*);*

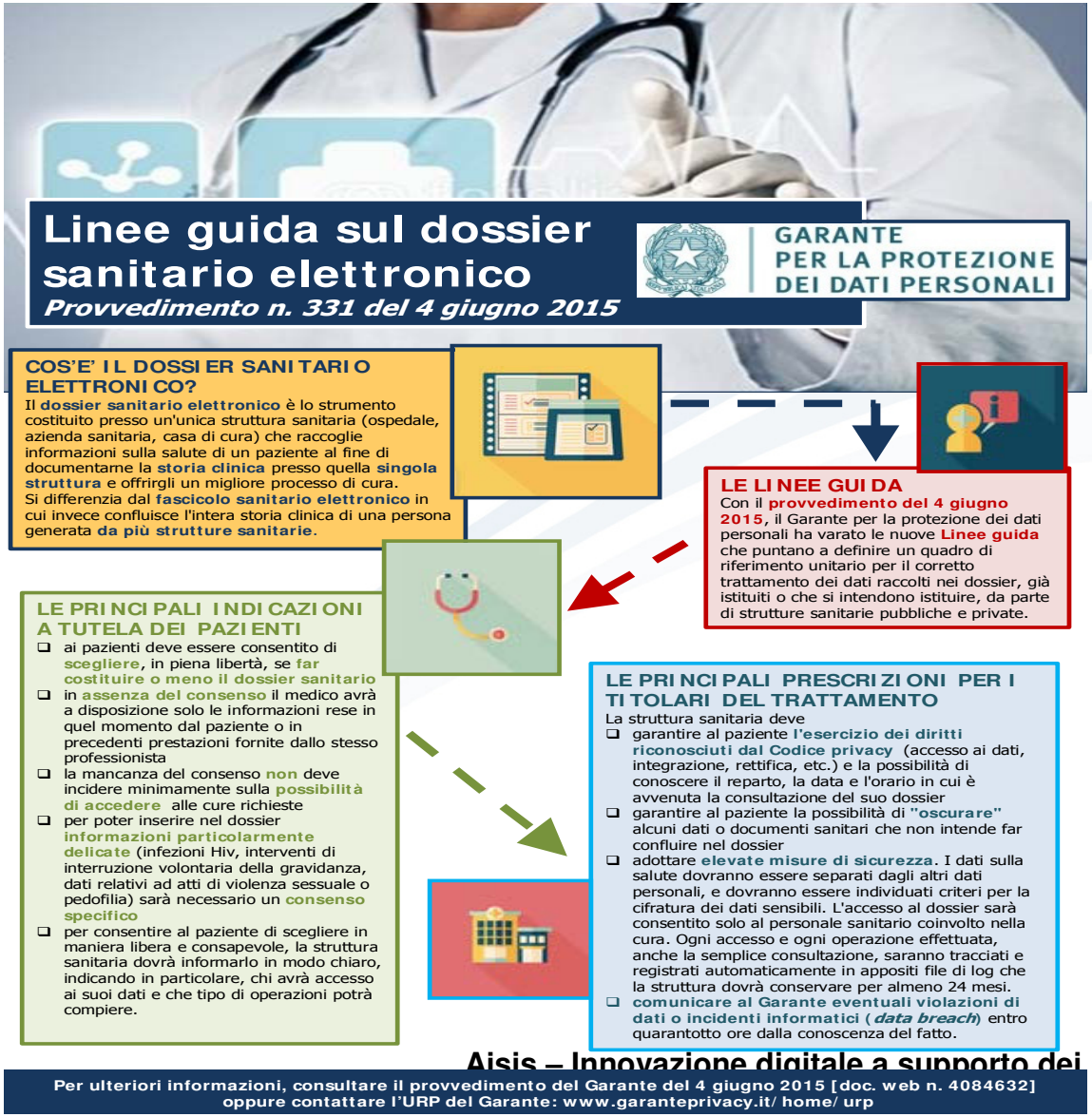
  - *"*Linee guida in tema di referti on-line*" del 19 novembre 2009, doc. web n. 1679033.*

- Secondo la definizione resa nelle Linee guida del 2009 il dossier sanitario è ***"lo strumento costituito presso un organismo sanitario in qualità <u>di unico titolare del trattamento</u>*** *(es., ospedale, azienda sanitaria, casa di cura)* ***al cui interno operino più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi*** *(es., referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso),* ***volte a documentarne la storia clinica****".*

- Il dossier sanitario raccoglie le informazioni relative agli eventi clinici occorsi all'interessato esclusivamente presso un'unica struttura sanitaria.

- In via principale, pertanto, **si differenzia dal Fse per la circostanza che <u>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,</u> come avviene proprio per il Fse.**

- Ciò stante, molte delle misure individuate a tutela della protezione dei dati in occasione dell'esame dei testi normativi relativi all'istituzione del **Fse** si ritiene debbano trovare applicazione anche con riferimento ai trattamenti effettuati mediante il dossier sanitario.



Con l'infografica il Garante ha rappresentato i principi fondamentali espressi delle Linee Guida. In linea generale, le linee guida contengono:

☐ **Le indicazioni a tutela del paziente** (come redigere l'informativa, come e quando raccogliere il consenso e consenso specifico, rilevanza della facoltatività dell'interessato a costituire il dossier sanitario, accesso al dossier)

☐ **Le prescrizioni per i Titolare del Trattamento** (riconoscimento del diritto all'oscuramento di dati e/o eventi clinici, e degli altri diritti dell'interessato, adottare elevate misure di sicurezza, comunicazione del data breach).

- Come già indicato dal Garante nelle *Linee guida* del 2009, la particolare delicatezza dei dati personali trattati mediante il *dossier* sanitario impone:
  - **Misure volte ad assicurare idonei livelli di sicurezza** (*art. 31 del Codice*);
  - **Misure minime di sicurezza** (*artt. 33 e ss.*);
    - 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.**
    - 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.
    - Aggiornamento periodico delle misure.

–La tracciabilità degli accessi e delle operazioni effettuate, anche di semplice consultazione (file di *log* degli accessi e delle operazioni compiute):

- realizzare sistemi di controllo che prevedano la registrazione automatica in appositi **file di *log* degli accessi** e delle operazioni compiute.

- 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.**

- è necessario che siano tracciate anche le operazioni di semplice consultazione (*inquiry*).

- Il Garante **ritiene congruo** stabilire che i *log* delle operazioni siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.

–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*** (ad es., relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

- I controlli, come anticipato, devono comprendere anche verifiche: **a posteriori, a campione o a seguito di allarme derivante da sistemi di *alert* e di *anomaly detection*,** sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento.

- L'attività di controllo deve essere adeguatamente documentata.

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

- Da ultimo sempre in tema di sicurezza, la novità del 2015 introdotta dal Garante rispetto alle *Linee guida* del 2009, è il **data breach**. :
  - Si prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice che, entro quarantotto ore dalla conoscenza del fatto, i titolari comunichino 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.
  - Tali comunicazioni devono essere redatte secondo lo schema riportato nell' **"Allegato B" ovvero il modello di comunicazione della violazione dei dati allegato** al provvedimento del 4 giugno 2015 e inviato tramite posta elettronica o posta elettronica certificata all'indirizzo: *databreach.dossier@pec.gpdp.it.*
  - La mancata comunicazione al Garante delle violazioni o degli incidenti informatici configura un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-*ter (da € 30.000,00 ai € 180.000,00)*, del Codice.
  - Comunicare infiene senza ritardo all'interessato le operazioni di trattamento illecito effettuate dagli incaricati o da chiunque sui dati personali trattati mediante il relativo dossier

• DIRITTO ALLA VISIONE DEGLI ACCESSI AL DOSSIER SANITARIO

– L'Autorità ritiene necessario, anche in coerenza con le previsioni normative in tema di Fse, di **riconoscere all'interessato il diritto alla visione degli accessi al proprio dossier sanitario**.

– **L'interessato può avanzare una formale richiesta al titolare del trattamento o a un suo delegato, al fine di 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**.

– Il titolare del trattamento o un suo delegato devono fornire riscontro alla suddetta richiesta dell'interessato **entro 15 giorni dal suo ricevimento**.

– Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o un suo delegato ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta medesima.

- **Il Fasciolo Sanitario Elettronico è istituito dalle Regioni e dalle Province Autonome**, nel rispetto della normativa vigente in materia di protezione dei dati personali per fini di:

  - **Prevenzione, diagnosi, cura e riabilitazione;**
  - **Studio e ricerca scientifica in ambito medico ed epidemiologico;**
  - **Programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.**

- **L'art. 12 del D. L. del 18 ottobre 2012, n. 179 – «Ulteriori misure per la crescita del paese»** ha definito il Fascicolo Sanitario Elettronico, come **«l'insieme di dati e di documenti digitali di tipo sanitario e socio - sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito».**

- Con il successivo D. L. n. 21 giugno 2013, n. 69 ***«Disposizioni urgenti per il rilancio dell'economica»*** che ha apportato modifiche al D.L. n. 179/2012, hanno stabilito quale termine per l'attivazione del FSE presso le Regioni e le Provincie Autonome **il 30 giugno 2015 (prorogato al 31 dicembre 2015** per l'interoperabilità tra Regione e Regione)

- Il Ministero della salute, al fine di dare **attuazione** alle disposizioni contenute nel comma 7 dell'articolo 12 del decreto legge n. 179 del 2012, e successive modificazioni, ha predisposto lo **schema di Decreto del Presidente Consiglio dei Ministri che disciplina nel dettaglio il fascicolo sanitario elettronico (FSE).**

- Lo schema di DPCM è stato trasmesso alla Presidenza del Consiglio dei Ministri ai fini del prosieguo dell'iter di adozione del decreto.

- Su tale DPCM sono stati, inoltre, acquisiti il parere della Conferenza Stato-Regioni il 13 marzo 2014, del Garante Privacy il 22 maggio 2014 e del Consiglio di Stato il 4 dicembre 2014; quindi è stato trasmesso all'ufficio legislativo della Presidenza del Consiglio dei Ministri ai fini dell'emanazione".

- **Lo scorso 3 settembre 2015 è arrivata la firma del Ministro Lorenzin.**
- **Si attende la pubblicazione in gazzetta ufficiale.**

- **La definizione do FSE, secondo il Garante nelle linee guida del 2009:**
  - **Fse è il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale** (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta).

Il trattamento dei dati contenuti del FSE deve perseguire finalità:

1. **Prevenzione, diagnosi, cura e riabilitazione**

2. **Amministrative** (eventuale) **strettamente connesse all'erogazione della prestazione sanitaria richiesta dall'interessato** (esempio, prenotazione e pagamento di una prestazione). In tal caso gli strumenti devono essere strutturati in modo che i **dati amministrativi siano separati dalle informazioni sanitarie**, prevedendo profili di abilitazione diversi per gli aventi accesso, in funzione delle operazioni consentite.

3. **Ricerca scientifica, epidemiologica o statica** (eventuali) possono avvenire in conformità alla normativa di settore.

Fascicolo Sanitario Elettronico, composizione ai sensi del **DPCM art. 2**:

•I contenuti del FSE sono rappresentati da un nucleo minimo di dati e documenti, nonché da dati e documenti integrativi che permettono di arricchire il FSE.

•Il nucleo minimo è costituito da:

- **Dati identificativi ed amministrativi dell'assistito;**
- **Referti;**
- **Verbali di pronto soccorso;**
- **Lettere di dimissioni;**
- **Profilo sanitari sintetico;**
- **Dossier farmaceutico;**
- **Consenso o diniego alla donazione di organi e tessuti.**

•I dati e documenti integrativi sono degli ulteriori componenti del FSE la cui alimentazione è funzione delle scelte regionali e materia di politica sanitaria e del livello di maturazione del processo di digitalizzazione.

IL DPCM contiene prescrizioni in ordine a:

- Dati soggetti a maggior tutela dell'anonimato (HIV, interruzione volontaria gravidanza, vittime di violenza sessuale e pedofilia ecc.);
- Informativa agli interessati e raccolta del consenso;
- Diritti dell'assistito;
- Accesso al FSE dell'assistito;
- Finalità di cura, ricerca e governo;
- Soggetti che concorrono all'alimentazione del FSE;
- Accesso alle informazioni per finalità di cura, ricerca e governo, anche in caso di emergenza;
- Regole tecniche e Misure di sicurezza

L'adozione del Fascicolo Sanitario Elettronico è FACOLTATIVA. Affinché tale scelta sia effettivamente libera, **l'interessato che non desideri che sia costituito un Fse deve poter accedere comunque alle prestazioni del Servizio sanitario nazionale** e non avere conseguenze negative sulla possibilità di usufruire di prestazioni mediche.

La sicurezza del FSE. Le prescrizioni del Garante e dell'art. 23 del DPCM.

La particolare delicatezza dei dati personali trattati mediante il Fse impone l'adozione:

- **Misure idonee di sicurezza (art. 31 del Codice);**

- **Misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).**

- **Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati** devono essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto **ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi** (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).

La sicurezza del FSE. Le prescrizioni del Garante e dell'art. 23 del DPCM.

- **Devono essere, inoltre, assicurati:**
  - **idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento** (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
  - **procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati**;
  - **Protocolli di comunicazione sicuri basati su standard crittografici** per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.
  - individuazione di **criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;**
  - **tracciabilità degli accessi e delle operazioni effettuate**;
  - **sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.**
  - **Procedure di anonimizzazione degli elementi identificativi diretti.**

L'art. 23 DPCM sul fascicolo sanitario elettronico, prevede ulteriori misure nella bozza:

- **Deve essere garantita la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività, sono pertanto adottate misure di continuità operativa e di disaster recovery ai sensi del CAD.**

- la conservazione dei documenti informatici dovrà essere sempre effettuata ai sensi degli artt. 43 e 44 del CAD e delle Regole tecniche, il processo di conservazione potrà essere **affidato, in modo totale o parziale, a conservatori, pubblici o privati, che offrano adeguate garanzie organizzative e tecnologiche e previo accreditamento presso l'Agenzia per l'Italia Digitale (AgID) ai sensi dell'art. 44-bis del CAD.**

- **La struttura e l'organizzazione dei dati contenuti nel FSE deve garantire oltre alla differenziata organizzazione di tipologie di informazioni sanitarie in relazione alle finalità per cui vengono trattate, anche quella relativa ai diversi livelli di autorizzazione.**

- **In caso di violazioni tali da comportare la perdita, distruzione o la diffusione indebita di dati personali, il titolare del trattamento effettua una segnalazione all'Autorità garante per la protezione dei dati personali entro una settimana dal verificarsi dell'evento.**