Note interpretative alle Linee Guida del Garante Privacy per la corretta gestione del Dossier Sanitario Elettronico

Sommario

Sommario 1
1. Premessa 1
2. Normativa e documenti di riferimento 2
3. Scopo e ambito di applicazione 3
4. Definizioni 3
5. Il Dossier Sanitario Elettronico in Emilia Romagna 6
6. Informativa al dossier 8
7. Consenso al dossier 10
7.1 Particolari casi di consenso 11
7.2 Libera professione intramuraria 12
8. Accesso al dossier 12
8.1. Accesso giustificato al dossier 14
8.2. Finalità particolari di accesso al dossier 16
9. Diritti dell'interessato 17
9.1 Diritto all'oscuramento 17
9.2 Diritto alla visione degli accessi al dossier 19
10. Sicurezza dei dati 19
10.1 Responsabili e Incaricati 20
10.2 Sistemi di autenticazione e di autorizzazione 20
10.3 Tracciabilità degli accessi e delle operazioni effettuate 21
10.4 Sistemi di audit log 21
10.5 Data Breach 22
11. Data protection officer (referente per la protezione dati) 23
12. Indicazioni per l'accesso al dossier di altre aziende in ambito provinciale 23

1. Premessa

Nel corso degli ultimi anni le aziende sanitarie e la Regione Emilia Romagna hanno implementato e innovato i loro sistemi informativi sanitari allo scopo di migliorare l'efficienza e l'efficacia delle cure dei pazienti; tali innovazioni tecnologiche, in particolare, hanno consentito a più organismi sanitari o a più professionisti di condividere informaticamente i dati di salute di un medesimo individuo e quindi di consultare in modo più veloce e diretto la storia clinica dei pazienti, con indubbi miglioramenti nel processo di cura dei pazienti stessi, nonché nella riduzione dei costi della spesa sanitaria derivanti, ad esempio, dalla ripetizione di esami.

Il Fascicolo Sanitario Elettronico (FSE) e il Dossier Sanitario Elettronico (DSE) rappresentano i due principali strumenti che hanno permesso la concreta realizzazione dell'archiviazione e della condivisione on-line dei documenti sanitari.

In Emilia Romagna la realizzazione del FSE è stata possibile grazie a SOLE (Sanità On Line), la rete informatica che già dal 2005 collega i medici di medicina generale e i pediatri di libera scelta a tutte le strutture sanitarie e agli specialisti del Servizio Sanitario

Regionale che possono condividere, se l'interessato ha dato il proprio consenso e nel rigoroso rispetto della privacy, la documentazione clinica relativa a prestazioni e servizi erogati nelle strutture del Servizio Sanitario Regionale.

Il DSE, in quanto strumento di titolarità dell'azienda, ha avuto uno sviluppo non omogeneo e localizzato nei diversi e specifici contesti, talvolta a seguito di iniziative sperimentali di informatizzazione in grado di gestire potenzialmente l'intera storia clinica del paziente.

Ne deriva che anche l'applicazione della normativa, diversamente interpretata dalle singole aziende, risenta delle specificità degli applicativi utilizzati e dell'organizzazione aziendale.

Inoltre dai recenti accertamenti ispettivi realizzati dall'Autorità Garante per la protezione dei dati personali sul DSE, che hanno interessato anche l'Emilia Romagna, sono state evidenziate le criticità nella sua implementazione rispetto alla complessità della disciplina sul trattamento dei dati, tali da suggerire un'attività di sensibilizzazione da parte della Regione nei confronti di tutte le aziende sulle cautele da adottare in caso di costituzione del DSE [1]

2. Normativa e documenti di riferimento

- *Legge 29 luglio 1975, n. 405 "Istituzione dei consultori familiari"*
- *Legge 22 maggio 1978, n. 194 "Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza"*
- *Legge 5 giugno 1990, n. 135 "Piano degli interventi urgenti in materia di prevenzione e lotta all'AIDS"*
- *D.P.R. 9 ottobre 1990, n. 309 "Testo Unico sulla droga"*
- *Legge 15 febbraio 1996, n. 66 "Norme contro la violenza sessuale"*
- *Legge 3 agosto 1998, n. 269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù"*
- *DM 16 luglio 2001, n. 349 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"*
- *Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*
- *Legge 6 febbraio 2006, n. 38* "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*

---

1 cfr. Relazione Garante del 2014 - Cap. 6 "Sanità"

- *Legge 17 dicembre 2012 n, 221 “Conversione, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese”*
- *DPCM 29 settembre 2015 n. 178 “Regolamento in materia di Fascicolo sanitario elettronico”*
- *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009*
- *Provvedimento Garante Privacy n. 3 del 10/01/2013 “Dossier sanitario e trattamento dei dati personali dei pazienti”*
- *Provvedimento Garante Privacy n. 340 del 3/07/2014 “Trattamento di dati tramite il dossier sanitario aziendale”*
- *Provvedimento Garante Privacy n. 468 del 23/10/2014 “Dossier sanitario elettronico e privacy dei pazienti”*
- *Provvedimento Garante Privacy n. 610 del 18/12/2014 “Illiceità nel trattamento di dati personali e sensibili presso una struttura ospedaliera”*
- *Provvedimento Garante Privacy n. 331 del 4/6/2015 “Linee guida in materia di Dossier sanitario”*
- *Provvedimento Garante Privacy n. 550 Dossier sanitario: prescrizioni per il sistema informativo delle prestazioni sanitarie erogate da un'Azienda sanitaria - 22 ottobre 2015*
- ***Provvedimento Garante Privacy n. 273 Dossier sanitario elettronico e trattamento di dati personali da parte di un'azienda ospedaliera - 22 giugno 2016***

3. Scopo e ambito di applicazione

Scopo del presente documento è dunque quello di fornire alle aziende sanitarie e alle strutture sanitarie del SSR indicazioni interpretative ed applicative delle Linee guida in tema di dossier sanitario elettronico, in modo da garantirne uno sviluppo quanto più uniforme su tutto il territorio regionale.

Il presente documento, senza pretese di completezza, vuole quindi rappresentare uno strumento di supporto alla applicazione delle regole sulla privacy in tema di DSE, relativamente alle finalità di prevenzione, diagnosi, cura e riabilitazione all'interno delle strutture sanitarie della Regione.

4. Definizioni

Applicativo verticale dipartimentale: sistema applicativo contenente le sole 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.

Consenso al dossier: la manifestazione di volontà dell'interessato o del suo rappresentante legale espressa liberamente, specificamente ed in modo informato con riferimento al trattamento dei dati personali effettuato mediante il dossier sanitario; tale consenso può essere manifestato in forma scritta o 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.

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati soggetti a maggiore tutela dell'anonimato (c.d. ultrasensibili): i dati personali disciplinati dalle disposizioni normative a tutela delle persone sieropositive, delle donne che si sottopongono a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari.

***Dossier Sanitario Elettronico (DSE)*:** insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica dai professionisti sanitari che lo assistono, al fine di documentarne la storia clinica e di offrirgli un migliore processo di cura. Tale strumento è costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. azienda sanitaria) al cui interno operino più professionisti;

Fascicolo Sanitario Elettronico (FSE): insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito

***Finalità amministrative correlate alla cura*:** finalità amministrative strettamente connesse all'attività di cura, che precedono, seguono o accompagnano l'attività assistenziale in senso stretto.

Finalità di cura: le finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato.

Finalità di ricerca: le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico.

Informativa al dossier: le informazioni che devono essere previamente fornite all'interessato o alla persona presso la quale sono raccolti i dati personali con riferimento al trattamento dei dati personali effettuato mediante il dossier***.***

LIS: applicativo dipartimentale verticale di laboratorio

Oscuramento**:** possibilità, su richiesta dell'interessato, di non far confluire nel DSE e nel FSE alcune informazioni sanitarie relative a singoli eventi clinici (ad es., con riferimento all'esito di una specifica visita specialistica o alla prescrizione di un farmaco). Ciò, analogamente a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di certi eventi.

Oscuramento dell'oscuramento: modalità tecnica che deve garantire, almeno in prima battuta, che tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato la scelta di oscurare uno o più eventi della sua storia clinica.

PACS: applicativo dipartimentale verticale per la gestione delle immagini diagnostiche (Picture Archiving Computed System); è usualmente integrato al RIS

Presa in carico**:** periodo di tempo in cui si articola il processo di cura. Il concetto di presa in carico viene esteso a tutte quelle fattispecie in cui il paziente è comunque in carico ad un certo professionista, o ad una certa équipe, o ad una certa struttura per un episodio o percorso di cura. In questo documento si considerano pertanto sovrapponibili i concetti di contatto/episodio/percorso di cura/presa in carico e si forniscono indicazioni di massima in merito al loro lasso temporale (vedi paragrafo 8).

Profondità dell'accesso: modalità di trattamento dei dati contenuti all'interno del dossier secondo limitazioni temporali e di contesto (ad esempio adottando un'organizzazione modulare dei dati) che consentono l'accesso da parte del personale preposto all'utilizzo del DSE ai soli dati indispensabili e pertinenti per svolgere i compiti ad essi demandati.

Prossimo congiunto: ai sensi dell'art. 307 del Codice Penale, si definiscono prossimi congiunti gli ascendenti, i discendenti, il coniuge, i fratelli, le sorelle, gli zii, i nipoti e gli affini nello stesso grado purché non sia morto il coniuge e non vi sia prole.

Rappresentante legale: è il soggetto che, per legge, agisce per conto del soggetto incapace di agire. Rappresentanti legali sono: l'esercente la responsabilità genitoriale, il tutore, il curatore, e l'amministratore di sostegno.

RIS: applicativo dipartimentale verticale di radiologia; è usualmente integrato al RIS

Soggetto incapace di agire: la capacità di agire, ai sensi dell'art. 2 del Codice Civile,

consiste nell'attitudine di un soggetto ad esprimere validamente la propria volontà ai fini giuridici. Soggetti incapaci di agire sono: i minorenni, gli interdetti (legali o giudiziali) e gli inabilitati.

Soggetto incapace di intendere o di volere: l'incapacità di intendere o di volere, cd. incapacità naturale, è uno *status* momentaneo, contingente e non abituale di incapacità che si determina per una qualsiasi causa che incide sulla sfera psichica e/o fisica di un soggetto. La stessa rileva solo nell'ipotesi in cui il soggetto agente abbia capacità legale di agire, ma sia privo, in una determinato momento, della capacità di intendere o di volere. In particolare, l'incapacità di intendere indica l'incapacità del soggetto a rendersi conto del significato delle proprie azioni; l'incapacità di volere, invece, indica l'incapacità di autodeterminarsi liberamente.

5. Il Dossier Sanitario Elettronico in Emilia Romagna

In mancanza di una definizione normativa a livello nazionale di dossier sanitario, coerentemente con le indicazioni dell'Autorità Garante, la Regione, al fine di fornire un'interpretazione che integri ed uniformi a livello regionale la descrizione di DSE definisce il DSE come lo strumento informatico interno alla struttura sanitaria (che è titolare del trattamento dei dati in esso contenuti) che raccoglie l'insieme degli eventi clinici erogati per il singolo assistito presso la struttura stessa e volto a documentarne in tale contesto, e in prospettiva, l'intera storia clinica.

Il DSE è da intendersi come strumento unico presso la struttura, che in prospettiva consenta ai professionisti sanitari della struttura stessa, coinvolti nel processo di cura, l'accesso all'insieme di tutte le informazioni disponibili, presenti ed eventualmente passate, inerenti lo stato di salute dei pazienti in carico che abbiano espresso gli adeguati consensi.

In particolare, si sottolinea che, in coerenza con i recenti sviluppi delle politiche nazionali e regionali e con gli interventi dell'Autorità Garante in tema di DSE e FSE, il DSE deve tendere a fornire accesso alla documentazione minima prevista dalla Rete SOLE:

- referti di laboratorio;
- referti di diagnostica per immagini;
- referti di attività di specialistica ambulatoriale;
- verbali/referti di pronto soccorso;
- lettere di dimissione ospedaliera

La complessità dei sistemi informativi sanitari utilizzati sul territorio regionale e la differente configurazione degli stessi in contesti diversi hanno progressivamente generato sistemi informativi potenzialmente utilizzabili anche come DSE. E' necessario quindi che le strutture sanitarie pongano particolare attenzione nell'individuare e adeguare la

destinazione d'uso propria del singolo applicativo dipartimentale verticale, evitando una qualificazione dello stesso come DSE.

Infatti, è da ritenersi quale corretta destinazione d'uso di un sistema come DSE la sussistenza contemporanea di due condizioni:

- accesso al sistema da parte di una pluralità di figure professionali afferenti a specialità anche diverse da quelle che hanno generato le informazioni in esso contenute;
- accesso a informazioni non limitato al solo episodio/accesso corrente.

Pertanto, al fine di evitare che taluni applicativi dipartimentali verticali vengano impropriamente a configurarsi come DSE, è necessario, in alternativa:

- l'adozione dello stesso applicativo dipartimentale verticale come DSE, con conseguente adeguamento alle indicazioni dell' Autorità Garante;
- oppure l'utilizzo dello/degli applicativo/i dipartimentale verticale solo come dipartimentale, con conseguente adeguamento, che ne limiti in alternativa:
    - ✓ l'accessibilità da parte dei soli professionisti della specialità trattata nel dipartimentale
    - ✓ l'accesso alle sole informazioni relative all'episodio corrente o ad eventuali precedenti della medesima specialità

Esempi di applicativi dipartimentali verticali che **non** incorrono nel rischio di essere utilizzati come DSE:

- Un sistema LIS, RIS o PACS che consenta ai soli operatori sanitari della specialità trattata dall'applicativo dipartimentale verticale (rispettivamente laboratorio e diagnostica per immagini) di accedere senza limitazione temporale di presa in carico a tutti i referti dei pazienti prodotti dagli stessi, nei limiti della stretta indispensabilità dell'accesso al singolo documento;
- Un sistema di refertazione ambulatoriale che consenta l'accesso ai referti relativi ad episodi precedenti senza limitazioni temporali della sola specialità del professionista;
- Un sistema LIS, RIS o PACS che consenta a tutti i medici di una struttura di accedere ai referti relativi ai soli episodi/accessi correnti del paziente in carico;

Esempi di applicativi dipartimentali verticali che si configurerebbero come DSE:

- Un sistema LIS, RIS o PACS che consenta a tutti i medici di una struttura di accedere, senza limitazione temporale e svincolata dalla presa in carico del paziente, a tutti i referti di laboratorio o radiologia dello stesso;
- Un sistema di refertazione ambulatoriale che consenta a tutti i medici abilitati al sistema, senza distinzione di specialità, di accedere senza limitazione temporale e svincolata dalla presa in carico del paziente, a tutti i referti relativi ad episodi

precedenti.

Nel caso in cui nella struttura non sia presente un DSE, ovvero il cittadino non abbia acconsentito alla creazione dello stesso, il professionista che prende in carico il paziente avrà a disposizione solo le informazioni:

- fornite in quel momento dal paziente (ad es., raccolta dell'anamnesi ed eventuale valutazione della documentazione sanitaria presentata dallo stesso);
- disponibili nello/negli applicativo/i verticale dipartimentale relativamente al solo episodio/accesso corrente;
- disponibili nell'applicativo verticale dipartimentale che tratta la specialità del professionista, relative a precedenti prestazioni erogate dallo stesso professionista/équipe (es. stesso ambulatorio/reparto) e quindi senza limitazione temporale.

Il trattamento dei dati personali effettuato mediante il dossier differisce da quello relativo alla compilazione e tenuta della Cartella Clinica Informatizzata, intesa come lo strumento informativo finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente e ad un singolo episodio di ricovero.

Si precisa che qualora il sistema di "Cartella Clinica Informatizzata" permetta l'accesso a precedenti cartelle cliniche riferite a specialità diverse rispetto a quella del reparto che ha in carico il paziente, o permetta accesso a informazioni di altre specialità relative a precedenti contatti (anche ambulatoriali), è necessario che tale accesso sia veicolato dal consenso al DSE. Quindi, in assenza del DSE o di diniego alla costituzione del DSE, il sistema di Cartella Clinica Informatizzata potrà proporre solo le informazioni relative al medesimo episodio o ad altri episodi relativi alla medesima specialità.

6. Informativa al dossier

Il trattamento dei dati personali effettuato tramite il dossier costituisce dunque un trattamento ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento per il quale l'interessato si rivolge ad esso. In assenza del dossier sanitario infatti, il professionista, come già evidenziato, ha 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 l'uso del dossier sanitario, invece, il professionista pone in essere un **ulteriore trattamento di dati sanitari** mediante la consultazione delle informazioni elaborate nell'ambito dell'intera struttura sanitaria e non solo del suo reparto/ambulatorio e, quindi, da professionisti/équipe diversi, in occasione di altri eventi clinici occorsi in passato all'interessato e riferibili anche a patologie differenti rispetto

all’evento clinico in relazione al quale l’interessato riceve la prestazione sanitaria.

In quanto tale, il trattamento dei dati personali effettuato mediante il dossier sanitario necessita di una **specifica informativa** che contenga oltre a tutti gli elementi previsti dall’art. 13 del Codice Privacy, anche quanto indicato dalle Linee guida del Garante relativamente a:

- **descrizione del dossier sanitario**: devono essere evidenziate le finalità e i vantaggi del dossier sanitario quale strumento fondamentale per il miglioramento della qualità e della personalizzazione delle cure, l’alleggerimento dell’onere documentale e la fruibilità immediata delle informazioni cliniche da parte dei professionisti sanitari. Deve essere altresì evidenziato che l’eventuale mancato consenso al trattamento dei dati mediante DSE non incide sulla possibilità di accedere alle cure mediche, in quanto, per definizione, tale strumento ha natura facoltativa. Una particolare attenzione deve essere riservata al trattamento dei dati c.d. ultrasensibili (v. paragrafo 7.1).
- **ambito di conoscibilità:** L’interessato deve essere informato in merito ai soggetti o alle categorie di soggetti ai quali i dati personali trattati mediante il dossier possono essere comunicati 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 (artt. 13, comma 1, lett. d), 22, comma 8, e 26, comma 5, del Codice). Tale strumento potrà essere, infatti, consultato nella sua interezza solo da parte dei professionisti sanitari che forniranno nel tempo e a vario titolo assistenza sanitaria al paziente.

  È inoltre necessario che sia specificata l’eventualità che il dossier sanitario sia consultabile anche da parte dei professionisti che agiscono in libera professione intramuraria. Infine deve essere resa 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 quando ciò sia ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività;
- **diritti dell’interessato**: devono essere indicate le modalità attraverso le quali l’interessato può rivolgersi al titolare e/o al responsabile per esercitare i diritti di cui agli artt. 7 e ss del Codice Privacy, le modalità per revocare il consenso, per esercitare l’eventuale facoltà di oscurare alcuni eventi clinici e le modalità per visionare gli accessi effettuati al DSE;

  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, ad esempio pubblicandola sul proprio sito Internet o affiggendola nei locali di attesa. Si evidenzia, infine, che in caso di omessa o inidonea informativa all'interessato è prevista una sanzione amministrativa (art. 161 del Codice).

7. Consenso al dossier

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 (artt. 18, comma 4, 23, 26, 76, 81 e 82 del Codice) in quanto all'interessato deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario.

Il consenso al DSE può essere acquisito in forma scritta o orale mediante annotazione, anche informatica, della dichiarazione espressa dal paziente. Titolato a esprimere il consenso è l'interessato ovvero, in caso di impossibilità fisica o incapacità di agire o incapacità di intendere o volere dello stesso, chi ne esercita legalmente la potestà, o un prossimo congiunto o un familiare o convivente o, in loro assenza, il responsabile della struttura presso cui l'interessato dimori.

Per quanto riguarda il minore, deve essere prevista l'acquisizione di un nuovo consenso al raggiungimento della maggiore età.

L'acquisizione del consenso al DSE deve essere effettuata una sola volta e la sua validità è estesa a tutta l'azienda. Pertanto, in ipotesi di avvenuta costituzione, il DSE sarà accessibile da parte di tutti i professionisti che, nel corso del tempo, interverranno nel processo di cura del paziente, senza la necessità che quest'ultimo manifesti tale volontà ogni volta che per vari motivi acceda alla struttura sanitaria.

Il consenso va declinato come segue:

1) diniego alla costituzione del dossier sanitario;
2) consenso alla costituzione del dossier sanitario ad esclusione dello storico (ovvero nel DSE non confluiranno episodi clinici precedenti alla sua data di costituzione);
3) consenso alla costituzione del dossier sanitario anche per lo storico (ovvero nel DSE confluiranno anche episodi clinici precedenti alla sua data di costituzione);
4) consenso all'inserimento nel dossier sanitario dei dati ultrasensibili; tale consenso sarà raccolto unitamente a quello di cui al precedente punto 3), cioè nel momento in cui il paziente acconsenta all'inserimento nel dossier sanitario anche dello storico e,

in seguito, ogniqualvolta venga erogata una prestazione sanitaria che comporti il trattamento di tali tipologie di dati.

(vedi a tal proposito anche il paragrafo 7.1).

Qualora si configuri l'ipotesi n. 1) o n. 2) è opportuno che venga spiegato chiaramente al paziente che con il diniego alla costituzione del dossier o all'inserimento dello storico, ferma restando la possibilità di accedere alle cure, egli rinuncia al vantaggio offerto da tale strumento in quanto, non potendo accedere informaticamente ai precedenti, i professionisti sanitari potrebbero non venire a conoscenza di tutte le informazioni necessarie per formulare la migliore strategia diagnostica o di cura con relative possibili conseguenze da un punto di vista clinico. Infine il consenso rilasciato può essere **revocato** liberamente in qualsiasi momento. In tale ipotesi, il DSE non sarà ulteriormente implementato e i dati sanitari in esso presenti rimarranno visibili unicamente al professionista che li ha redatti e per eventuali conservazioni per obbligo di legge (art. 22, comma 5, del Codice), ma non saranno più condivisi con i professionisti degli altri reparti che prenderanno in seguito in cura il paziente. Anche le modalità operative per richiedere la revoca del consenso dovranno essere rese note nell'informativa.

7.1 Particolari casi di consenso

Qualora Il titolare del trattamento decida di inserire nel dossier anche 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 (dati ultrasensibili) **occorre acquisire un autonomo e specifico consenso dell'interessato**. Si tratta, in particolare, dei dati soggetti a maggiore tutela dell'anonimato, ovvero relativi ad atti di violenza sessuale o di pedofilia, all'infezione da HIV o all'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari.

Come esposto nel paragrafo precedente, tale ulteriore autonomo e specifico consenso può essere raccolto unitamente a quello relativo all'inserimento dello storico nel dossier e, successivamente, in occasione dell'erogazione della specifica prestazione sanitaria che comporti il trattamento di dati ultrasensibili.

E' pertanto opportuno che l'informativa espliciti chiaramente all'interessato che, in caso di consenso all'inserimento dello storico, anche i suoi dati ultrasensibili entreranno a far parte del suo DSE.

Ferma restando l'indubbia utilità di un dossier completo, il titolare del trattamento può anche decidere di non rendere disponibili tali informazioni nel dossier configurando i possibili vincoli informatici nei singoli applicativi dipartimentali verticali (c.d. oscuramento di default). In tale ipotesi il dato ultrasensibile rimarrà solo a disposizione del professionista/équipe che l'ha generato.

Considerato che è possibile riconoscere alla fonte tipologie documentali che contengono dati ultrasensibili in modo automatico solo quando associati ad una specifica codifica (es. referti di laboratorio HIV, lettere di dimissioni IVG, ecc) e quindi prevedere per essi un oscuramento di default, resta inteso che negli altri casi, ossia nelle ipotesi in cui le informazioni ultrasensibili siano riportate in documenti di altro tipo (es. verbale di PS), è opportuno che i sistemi informativi consentano al medico refertante di oscurare il documento oppure di annotare lo specifico consenso richiesto al paziente per l'inserimento nel suo DSE di tali informazioni ultrasensibili. Tale previsione viene richiamata per il FSE all'art. 5, comma 1 e 2 del decreto del Presidente del Consiglio dei ministri 29 settembre 2015 n. 178 "Regolamento in materia di Fascicolo sanitario elettronico".

7.2 Libera professione intramuraria

Quando nell'informativa è specificata l'eventualità che il DSE sia consultabile da parte dei professionisti che agiscono in libera professione intramuraria – detta anche intramoenia – occorre acquisire da parte del professionista che eroga la prestazione un consenso specifico.

8. Accesso al dossier

Il dossier sanitario costituisce uno strumento di ausilio per il personale sanitario consultabile da parte dello stesso nel processo di cura del paziente: la finalità primaria perseguita attraverso tale strumento è, pertanto, quella di prevenzione, diagnosi, cura e riabilitazione dell'interessato. In quanto tale, l'accesso al dossier deve essere limitato al personale sanitario che interviene nel tempo nel processo di cura del paziente e deve essere posto in essere esclusivamente da parte dei soggetti operanti in ambito sanitario.

Per personale sanitario si intendono i professionisti/équipe preposti alla cura dell'interessato (medici, case manager, infermieri, ostetriche, biologi…); è compito dell'azienda individuare ed implementare le regole tecniche idonee per gestire la c.d. "profondità dell'accesso", in base ai diversi profili di autenticazione al dossier.

Il "personale sanitario" è costituito dalle "professioni sanitarie" riconosciute dal Ministero della Salute, il cui elenco aggiornato è pubblicato sul portale internet del Ministero, che necessitano dell'iscrizione a un albo professionale e sono

deontologicamente tenute al rispetto della riservatezza e vincolate alla segretezza delle informazioni e dei dati trattati nell'ambito dei processi di diagnosi e cura.

L'insieme di professioni sanitarie e le competenze multidisciplinari che interagiscono nel percorso del paziente, costituiscono il "personale che ha in cura il paziente"
Accanto al personale strutturato, assume rilevanza il ruolo di coloro che in quanto iscritti alle Scuole di specializzazione universitarie, partecipano, nell'ambito del percorso di formazione, ai processi di diagnosi e cura.
I relativi "Tutor" sono individuati tra il personale sanitario, indirizzando le azioni del laureato in formazione specialistica.
In ogni caso i laureati di area sanitaria, specializzandi, devono essere nominati incaricati del trattamento e sono soggetti al vincolo di riservatezza e al segreto professionale che riguarda tutti coloro che, indipendentemente dal profilo professionale e dal ruolo operativo, collaborano nella gestione del paziente nel percorso di diagnosi e cura.
Le medesime considerazioni valgono per le ulteriori figure quali, dottorandi e dottori di ricerca, frequentatori e tirocinanti.
Spetta alla singola Azienda, nell'ambito dell'autonomia organizzativa, e in qualità di Titolare del dato, definire, con proprio regolamento, per ciascuna figura strutturata e non, il profilo di autorizzazione e l'ambito di trattamento consentito.
L'accesso al DSE *"limitatamente al tempo in cui si articola la presa in carico del paziente*" si traduce mettendo automaticamente a disposizione del professionista sanitario i dossier dei pazienti che sono in quel momento in cura presso lo stesso (ad es., medico di reparto rispetto ai dossier relativi ai pazienti ricoverati; medico che opera in ambulatorio rispetto ai dossier dei soggetti a cui in quel giorno deve essere erogata la prestazione ambulatoriale), ferma restando la possibilità di accedere nuovamente al dossier (c.d. accesso giustificato v. par. 8.1.) qualora ciò si renda necessario in merito al tipo di trattamento medico da prestare all'interessato.
A tal fine, allo scopo di agevolare i professionisti sanitari nella consultazione del dossier, si suggerisce di adottare modalità automatiche di prese in carico nei casi in cui gli accessi risultino registrati informaticamente negli applicativi dipartimentali verticali o nel DSE. Da tali automatismi, che devono essere implementati nel rispetto dei principi di pertinenza e non eccedenza, ne consegue che il periodo di tempo in cui si articola il processo di cura del paziente possa essere individuato precisamente, ad esempio, come segue:

- **regime di ricovero ordinario e day hospital**: il professionista sanitario può consultare il dossier dall'inserimento del paziente nella lista d'attesa o dall'accettazione e ne conserva la visibilità anche dopo la data di dimissione. Tale accesso rimane garantito senza necessità di giustificazione, a seconda dell'organizzazione aziendale e dei percorsi/programmi di cura in essere per un periodo che può variare da 1 mese a 3 mesi dalla dimissione.
- **regime ambulatoriale e day service**: il professionista sanitario può consultare il dossier dal momento dell'accettazione del paziente e anche successivamente alla validazione del referto o alla chiusura dell'episodio. Tale accesso rimane garantito senza necessità di giustificazione, a seconda dell'organizzazione aziendale e dei percorsi/programmi di cura in essere, per un periodo che non può superare un mese dalla validazione del referto o dalla chiusura dell'episodio.
- **regime di Pronto Soccorso**: il professionista sanitario può consultare il dossier dal momento dell'accettazione del paziente e anche successivamente alla validazione del referto o alla chiusura dell'episodio. Tale accesso rimane garantito senza necessità di giustificazione, a seconda dell'organizzazione aziendale e dei percorsi/programmi di cura in essere, per un periodo che non può superare una settimana dalla validazione del referto o dalla chiusura dell'episodio, potendo anche coincidere con la chiusura dell'episodio stesso.

Il periodo di latenza individuato dalle singole aziende per ogni regime, dovrà essere motivato e definito preventivamente per poi essere implementato nel DSE.

E' altresì auspicabile la formalizzazione informatica dello stato di paziente cronico (ad es. diabete, scompenso) e dei percorsi di cura compositi (ad es. gravidanza, dipendenze) che non rientrano nei casi precedenti. Tale formalizzazione consentirebbe di attribuire informaticamente la condizione di "paziente in carico" riducendo l'utilizzo dell'accesso giustificato.
Ad oggi si consiglia di utilizzare quale motivazione per l'accesso giustificato quella relativa al completamento del percorso diagnostico – terapeutico.

8.1. Accesso giustificato al dossier

Nella consapevolezza che non è possibile prevedere in modo rigido e statico la casistica reale delle pratiche cliniche articolate su un periodo di presa in carico definito e registrato informaticamente e che per giustificati motivi può richiedere la possibilità di accedere nuovamente al dossier qualora ciò si renda necessario in merito al tipo di trattamento

medico da prestare all'interessato (ad es. accesso in consulenza o per revisione di casi), il DSE deve consentire un accesso ai dati di pazienti anche oltre gli automatismi informatici di presa in carico.

Tali accessi c.d. "giustificati" devono avvenire sulla base di una casistica predeterminata dall'azienda tramite una ricerca libera anagrafica del paziente che ha espresso il consenso al DSE. Si consiglia di limitarne l'uso ai soli professionisti medici.

Le motivazioni da prevedere sono ad esempio:

- **attività di consulenza**: il professionista non ha in carico il paziente, ma deve effettuare attività di consulenza sanitaria nell'interesse di quest'ultimo (es. il paziente è ricoverato e c'è necessità di chiedere una consulenza ad un'altra U.O.);
- **completamento del percorso diagnostico - terapeutico**: il professionista aveva in carico il paziente, ma è decorso il termine di visibilità definito per quel caso e lo stesso ha necessità di accedere nuovamente al DSE per verificare il tipo di trattamento medico da prestare all'interessato (es. il paziente rivolge al medico una richiesta di chiarimenti terapeutici);
- **accessi/percorsi non registrati informaticamente**: per ambiti in cui la presa in carico non è informatizzata o in caso di indisponibilità degli applicativi verticali dipartimentali (es. guasto ADT);
- **prelievi/trapianti**: utilizzabile quando vengono compiute attività connesse alla valutazione dell'idoneità del donatore per l'espianto e il successivo trapianto**;**
- **salvaguardia di un terzo o della collettività**: utilizzabile quando sia ritenuto indispensabile consultare il dossier per la tutela di un terzo e della collettività (es. condivisione di ambienti con l'interessato per rischi di contagio/infezioni);
- **rivalutazione di casi chiusi:** utilizzabile quando il medico ha la necessità di rivedere quel caso specifico anche alla luce di nuove esigenze cliniche;
- **ricoveri/percorsi gestiti con medici di guardia interdivisionali, medici reperibili su più reparti, ospedali gestiti per intensità di cura, letti di appoggio**: utilizzabile nei casi di dossier a cui deve accedere personale medico a cui informaticamente non può essere assegnato il paziente;
- **finalità di ricerca:** nel rispetto di quanto previsto dal Codice per tali tipi di trattamenti, ovvero, in via generale, previa acquisizione di un ulteriore specifico consenso informato del paziente (art. 110 del Codice).

8.2. Finalità particolari di accesso al dossier

Posta la regola generale, ossia che l'accesso al DSE nella sua interezza è finalizzato alle attività di prevenzione, diagnosi, cura e riabilitazione dell'interessato, può talvolta accadere che il personale amministrativo operante all'interno dell'azienda utilizzi il medesimo per acquisire i dati necessari all'assolvimento delle funzioni amministrative correlate alla cura (es. per adempiere ai debiti informativi istituzionali, con accesso limitato alle sole informazioni indispensabili ad assolvere agli stessi). In tali casi devono essere 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.

Tale organizzazione modulare è di fondamentale importanza in quanto, qualora non fossero previsti moduli distinti all'interno del dossier per l'esercizio delle suddette funzioni, l'utilizzo di tali strumenti, per l'assolvimento dei predetti debiti informativi, potrebbe portare al paradosso secondo cui, laddove l'interessato non abbia manifestato il proprio consenso al dossier sanitario o abbia esercitato l'oscuramento di alcuni dati o documenti, la struttura sanitaria non potrebbe assolvere al debito informativo previsto dalla legge. È necessario, pertanto, che il titolare del trattamento individui autonome modalità di acquisizione dei dati indispensabili ad assolvere a tali debiti informativi, ad esempio utilizzando le sole informazioni indispensabili generate dai singoli applicativi dipartimentali verticali.

In analogia, con riferimento alla quantità e qualità dei dati e alla presenza dei dati storici visibili ai fini dell'attività di gestione delle prenotazioni nel sistema Cup, occorre ridurre la visibilità ai soli dati indispensabili all'attività stessa, prevedendo un'organizzazione modulare differenziata, relativamente agli operatori di front office (es. prenotazione telefonica) e di back office (es. gestione delle agende, verifica mancata disdetta, ecc…).

Posto che l'identificazione dei soggetti o delle categorie dei soggetti abilitati a consultare il dossier deve essere effettuata con chiarezza dall'azienda si precisa che sono escluse dall'accesso al DSE le seguenti categorie di soggetti:

1. personale medico che agisce nell'esercizio di attività medico-legali in ambito certificatorio (ad es. visite per l'accertamento dell'idoneità lavorativa o per il rilascio di certificazioni necessarie al conferimento di permessi o abilitazioni);
2. periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario.

E' preclusa in ogni caso ogni forma di utilizzo, ancorché in forma aggregata e anonima, dei dati contenuti nei dossier - come peraltro in tutti gli applicativi - per finalità commerciali, a titolo oneroso o gratuito, ivi compresi gli accordi con società operanti nel settore farmaceutico.

9. Diritti dell'interessato

Il titolare del trattamento deve garantire che l'interessato possa esercitare nei confronti di tale trattamento i diritti indicati nell'art. 7 del Codice, che devono essere citati nell'informativa al DSE (vedi par. 6). In particolare, 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, comma 1 e 2, lett. a) e b), del Codice).

Quanto alle modalità implementative del trattamento dei dati attraverso il dossier sanitario, essendo questo un trattamento di dati personali effettuato con modalità elettroniche atte a consentire una forte integrazione di dati e documenti contenenti informazioni idonee a rivelare lo stato di salute, assume particolare rilievo il diritto riconosciuto all'interessato di poter ottenere l'indicazione della logica applicata a tale trattamento (art. 7, comma 2, lett. c), del Codice), ovvero l'indicazione dei criteri utilizzati nell'elaborazione elettronica dei dati.

Inoltre per quanto riguarda l'ambito di conoscibilità del DSE, l'interessato ha diritto di ottenere 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 (art. 7, comma 2, lett. e), del Codice).

Infine, qualora l'interessato richieda di integrare, rettificare, aggiornare i dati trattati mediante il dossier sanitario, trattandosi di documentazione medica, in analogia a quanto disposto dall'Autorità in tema di ricerche in ambito medico, biomedico ed epidemiologico, il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati deve essere fornito annotando le modifiche richieste senza alterare la documentazione di riferimento.

9.1 Diritto all'oscuramento

Un'importante garanzia a tutela della riservatezza dell'interessato che abbia manifestato la propria volontà in merito al trattamento dei dati personali mediante il dossier sanitario, consiste nella possibilità che lo stesso decida di oscurare taluni documenti sanitari consultabili tramite tale strumento, anche non contenenti dati ultrasensibili.

Tale garanzia, già indicata dal Garante nelle Linee guida del 2009, è stata riproposta dal legislatore anche con riferimento al FSE (cfr. art. 12, comma 3-bis, d.l. 18 ottobre 2012, n.

179 e art. 8, comma 1 e 2 del decreto del Presidente del Consiglio dei ministri 29 settembre 2015 n.178 “Regolamento in materia di Fascicolo sanitario elettronico”).

Ferma restando, infatti, l’indubbia utilità di un dossier sanitario il più possibile completo, il titolare del trattamento deve garantire la possibilità per l’interessato di non far confluire in esso alcune informazioni sanitarie. Al riguardo, come già evidenziato, si ricorda che di per sé il dossier sanitario costituisce uno strumento informativo incompleto.

È, inoltre, importante evidenziare che i dossier sanitari non certificano lo stato di salute dei pazienti, in quanto consistono in strumenti che possono aiutare il clinico ad inquadrare meglio e più rapidamente lo stato di salute di questi, nel rispetto del diritto-dovere del medico di effettuare gli accertamenti che riterrà - anche deontologicamente - più opportuni. Il titolare del trattamento è pertanto tenuto ad informare i soggetti abilitati ad accedere ai dossier in ordine alla possibilità che gli stessi possono non essere completi.

In relazione alle modalità tecniche di implementazione, la normativa prevede che l’oscuramento dell’evento clinico (revocabile nel tempo) debba avvenire in modo 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/équipe negli applicativi verticali dipartimentali che li ha raccolti o elaborati. Si precisa altresì che per oscuramento dell’evento deve intendersi non l’oscuramento di un dato all’interno del documento che lo contiene, in quanto trattandosi di documentazione sanitaria l’eliminazione di una parte risulterebbe esserne un’alterazione, ma l’oscuramento del singolo referto o altra tipologia documentale o, se esplicitato dall’interessato, di tutta la documentazione riferita ad un episodio/evento.

Ciò premesso, si condivide l’esigenza manifestata da più operatori del settore e da parte delle associazioni di pazienti di ben illustrare all’interessato l’utilità per l’operatore sanitario di disporre di un quadro clinico il più possibile completo della sua salute. In tal senso, devono essere compiutamente illustrate a quest’ultimo le conseguenze di detto oscuramento, nonché il significato clinico dell’informazione che si intende oscurare.

Per quanto riguarda l’eventuale modalità di gestione dell’oscuramento dei dati ultrasensibili si rinvia al paragrafo 7.1.

Infine si precisa che il titolare deve garantire l’esercizio di tale diritto sia al momento dell’erogazione della prestazione, sia successivamente attraverso le modalità organizzative e operative ritenute idonee (es. sottoscrizione di un apposito modulo da parte dell’interessato e successivo invio o presentazione all’ufficio competente a riceverlo).

9.2 Diritto alla visione degli accessi al dossier

Un’ulteriore garanzia che viene riconosciuta all’interessato a riprova delle corrette modalità impiegate nel trattamento dei suoi dati tramite il DSE è il riconoscimento del diritto alla visione degli accessi allo stesso.

Tale diritto rappresenta, in aggiunta al sistema di individuazione dei profili e dei livelli di autenticazione/accesso ai sistemi da parte degli utenti autorizzati, un’ulteriore misura di sicurezza finalizzata a monitorare ipotesi di accesso non autorizzato ai dati personali trattati mediante il DSE. In tal senso, in relazione al FSE si rinvia a quanto disposto dall’art. art. 13 com. 3 del DPCM 178/2015 in cui è previsto che ogni accesso alle informazioni contenute nel FSE sia registrato in apposita sezione a disposizione dell’assistito, che può prenderne visione in qualunque momento consultando il proprio Fascicolo per via telematica.

Relativamente all’esercizio di tale diritto sul DSE l’art. 154, comma 1, lett. c), del Codice prescrive ai titolari del trattamento di fornire all’interessato, un riscontro alla richiesta avanzata dallo stesso o da un suo delegato, volta a conoscere gli accessi eseguiti sul proprio dossier. Il riscontro da parte del titolare del trattamento dovrà indicare la struttura/reparto che ha effettuato l’accesso, la data e l’orario.

Di tale diritto esercitabile dagli interessati devono essere opportunamente informati anche i soggetti autorizzati ad accedere al dossier sanitario.

Analogamente a quanto previsto dal Codice per l’esercizio dei diritti di cui agli artt. 7 e ss., 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 trenta giorni dal ricevimento della richiesta medesima.

La richiesta di visione può riguardare accessi avvenuti nei due anni precedenti alla stessa.

10. Sicurezza dei dati

Data la natura dei dati trattati mediante il DSE, è necessaria, da parte del titolare del trattamento, l’adozione di specifici accorgimenti di natura organizzativa e tecnica, finalizzati a garantire idonei ed adeguati livelli di sicurezza, ferme restando le misure minime che ciascun titolare deve comunque adottare ai sensi del Codice Privacy.

10.1 Responsabili e Incaricati

A tal fine si ricorda come tutti i soggetti abilitati a trattare i dati personali mediante il DSE devono essere designati Incaricati del trattamento e devono essere adeguatamente istruiti in merito alle modalità di utilizzazione di tale strumento, nonché alle misure adottate per la tutela dei dati personali trattati mediante gli stessi. Il titolare ha inoltre la facoltà di designare eventuali soggetti quali “responsabili del trattamento”.

Il titolare o il responsabile, se designato, deve quindi indicare con chiarezza agli incaricati l’ambito del trattamento consentito, avendo cura di specificare la tipologia di operazioni agli stessi consentite (ad es., visualizzazione, visualizzazione con accesso giustificato, inserimento dati, ecc.) e le misure di sicurezza, sia logiche che fisiche, da rispettare nelle operazioni di trattamento.

Specifiche istruzioni, poi, devono essere rese a quei soggetti deputati ad accogliere le richieste di oscuramento, di visione degli accessi al dossier e di revoca del consenso.

Al riguardo, si evidenzia che la mancata designazione ad incaricati del trattamento non costituisce un mero inadempimento formale, in quanto gli incaricati, ponendo in essere una o più operazioni di trattamento dei dati personali, sono i soggetti che possono più facilmente incorrere nei rischi connessi al trattamento. In tal senso, è necessario che oltre alla formalizzazione di idonee istruzioni in merito al trattamento di dati personali effettuato mediante il dossier, siano resi consapevoli delle connesse responsabilità.

Si precisa, infine, che la mancata designazione ad incaricato del trattamento è idonea a configurare un illecito penale per l’omessa adozione delle misure minime di sicurezza (artt. 33 e ss. e 169 del Codice), nonché, in ogni caso, una fattispecie sanzionata amministrativamente (art. 162, comma 2- bis, del Codice).

Pur nella discrezionalità del singolo titolare del trattamento si consiglia di proporre attività di sensibilizzazione mediante formazione specifica o incontri a tema al fine di far meglio comprendere l’importanza di tale strumento e delle misure da adottarsi per la protezione dei dati personali con esso trattati.

Si ricordano inoltre gli adempimenti necessari relativi all’eventuale nomina di responsabili esterni e/o di amministratori di sistema.

10.2 Sistemi di autenticazione e di autorizzazione

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, amministrativo e tecnico/informatico. Le predette esigenze devono essere individuate sia sulla base di una specifica analisi del contesto

organizzativo della singola azienda, sia a seguito di un monitoraggio delle casistiche per le quali il personale ha necessità di consultare i dossier sanitari.

Tali sistemi devono consentire, come sopra ricordato, un accesso selettivo al dossier sanitario fondato sul principio di indispensabilità del dato trattato.

È necessario, inoltre, che il titolare individui procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati, ad esempio tramite la verifica annuale della loro sussistenza (All. B D.Lgs. 196/2003)

10.3 Tracciabilità degli accessi e delle operazioni effettuate

Al fine di strutturare un sistema di controllo delle operazioni effettuate sul DSE, il titolare del trattamento deve attivare, seppur in assenza di disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni e ferma restando la disciplina in materia di controllo a distanza dell'attività dei lavoratori, procedure che prevedono la registrazione automatica, in appositi file di log, degli accessi e delle operazioni compiute.

In particolare, i file di log devono registrare per ogni operazione di accesso al DSE effettuata da un incaricato, 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;
- la tipologia dell'operazione compiuta sui dati, compresa la semplice consultazione (inquiry).

In merito alla conservazione dei log, tenuto conto della indicazione data dal Garante nelle Linee guida del 2015 e in considerazione della disponibilità di un sistema di conservazione regionale adeguato ai grandi volumi di dati che nel tempo si generano, si ritiene opportuno che i log delle operazioni siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.

10.4 Sistemi di audit log

Il titolare del trattamento deve mettere in opera sistemi per il controllo degli accessi 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.

Occorre prefigurare, quindi, l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento, ad es.:

numero degli accessi eseguiti da parte di un singolo incaricato che utilizza la funzione “accesso giustificato” in un ambito temporale predefinito, numero di accessi eseguiti su uno specifico paziente….).

L’attività di controllo deve essere demandata a un’unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati sanitari dei pazienti.

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 (es. Ufficio Disciplinare, Direzione Sanitaria, Ufficio Privacy..) e messo a disposizione del Garante, in caso di specifica richiesta.

10.5 Data Breach

Le peculiari caratteristiche del trattamento dei dati effettuato mediante il DSE rendono necessario assoggettare il loro trattamento all’obbligo di comunicazione al Garante nel caso si verifichino violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware ecc.) che possano avere avuto un impatto significativo sui dati personali trattati attraverso il dossier.

A questo fine, ai sensi dell’art. 154, comma 1, lett. c), il titolare ha l’obbligo di comunicare al Garante per la protezione dei dati personali, entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

La comunicazione deve essere effettuata dal Data protection officer, dove presente, utilizzando lo schema riportato nell' Allegato B alle Linee guida sul DSE emanate dal Garante del 2015 e inviata tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.dossier@pec.gpdp.it.

In tali ipotesi, l’interessato sarà avvisato, senza ritardo, circa le operazioni di trattamento illecito effettuate dagli incaricati o da chiunque sui dati personali trattati mediante il relativo DSE, al fine di consentire allo stesso di minimizzare i rischi connessi alla violazione della disciplina di protezione dei dati personali.

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.

11. Data protection officer (referente per la protezione dati)

In ragione della particolare delicatezza delle informazioni trattate mediante il dossier sanitario, il Garante, già nelle Linee Guida sul DSE, auspicava che i titolari del trattamento individuassero al loro interno una figura di responsabile della protezione dei dati (c.d. DPO - data protection officer), con il ruolo di referente nei rapporti con il Garante, anche in relazione ai casi di data breach precedentemente illustrati.

Con l'emanazione del Regolamento UE 2016/679 del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, la previsione della nomina del responsabile della protezione dei dati diviene di fatto obbligatoria a partire dall'entrata in vigore del Regolamento stesso (25 maggio 2018).

12. Indicazioni per l’accesso al dossier di altre aziende in ambito provinciale

Sono sempre più numerose forme di necessaria condivisione di dati sanitari nell’ambito dell’organizzazione di attività integrate implementate su base provinciale allo scopo di migliorare l’efficacia della cura, l’efficienza dell’assistenza sanitaria e dell’appropriatezza anche al fine del contenimento della spesa.

Per consentire tale condivisione a professionisti che operano nell’ambito di diverse aziende e che intervengono in percorsi di cura integrati l’Autorità Garante ha recentemente affermato che “ove diverse strutture sanitarie che intervengono nel percorso di cura abbiano necessità di consultare i documenti clinici, in formato elettronico, di pazienti affetti da particolari patologie (es. rete oncologica) l'accesso ai diversi dossier sanitari è possibile, previa acquisizione dello specifico e ulteriore consenso informato dell'interessato” nelle medesime modalità previste da ciascuna azienda per il singolo dossier. Pertanto l’informativa, resa dal singolo Titolare del trattamento relativamente all’ambito di conoscibilità (cfr. par. 6) deve rendere evidente l’ambito di operatività del sistema dossier all’interno dei particolari percorsi individuati dalle singole aziende.

Resta inteso che con specifico riferimento all’accesso al dossier di un’altra azienda si richiama la necessità che siano realizzate misure a protezione dell’identità del paziente, siano utilizzati canali di comunicazione sicuri, siano adottati sistemi di autenticazione e autorizzazione che assicurino l’accesso selettivo ai dati in linea con i principi generali, integrando quanto definito relativamente alle operazioni di accesso nel par. 8.1.