GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

LINEE GUIDA IN MATERIA DI DOSSIER SANITARIO

Allegato A alla **deliberazione del Garante del 4 giugno 2015**

SOMMARIO

1. PREMESSA

Negli ultimi anni l'utilizzo di sistemi informativi per la gestione e la consultazione delle informazioni sanitarie relative alla storia clinica di un individuo ha trovato un'ampia diffusione nel settore sanitario sia nazionale che internazionale. Tale fenomeno è stato colto anche dal legislatore nazionale attraverso la previsione di una disciplina giuridica del Fascicolo sanitario elettronico (Fse) che si colloca all'interno di una crescente attenzione alla materia della sanità elettronica (art. 12, decreto legge 18 ottobre 2012, n. 179).

*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*), la refertazione* on-line *sono solo alcuni dei più recenti interventi normativi nel settore, rispetto ai quali le misure a tutela della protezione dei dati personali hanno costituito un importante momento di riflessione istituzionale (cfr. provvedimento del Garante "*Linee guida in tema di referti on-line*" del 19 novembre 2009, doc. web n. 1679033; decreto del Presidente del Consiglio dei Ministri dell'8 agosto 2013, pubblicato in G.U. Serie Generale n.243 del 16-10-2013, su cui il Garante ha espresso parere favorevole).*

Le politiche di sanità integrata che si stanno sviluppando sia in ambito nazionale che regionale considerano la condivisione delle informazioni sulla salute del paziente tra gli operatori sanitari uno strumento per rendere più efficienti i processi di diagnosi e cura dello stesso, nonché per ridurre i costi della spesa sanitaria derivanti, ad esempio, dalla ripetizione di esami clinici.

La sfida che tutti gli attori istituzionali sia nazionali che locali si pongono è, dunque, quella di garantire che i processi di integrazione dei dati sanitari assicurino un buon funzionamento dei sistemi clinici sia in termini di efficacia che di efficienza ed equità nel rispetto dei diritti fondamentali dell'individuo tra i quali si annovera quello alla tutela dei dati personali.

Affinché i dossier sanitari in uso presso le strutture sanitarie siano effettivamente degli strumenti di ausilio nei processi di diagnosi e cura dei pazienti è necessario che gli stessi siano realizzati con modalità tali da garantire in primo luogo la certezza dell'origine e della correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati. A questi aspetti sono connessi i principali rischi che il Garante ha potuto riscontrare nell'esame di numerosi dossier sanitari oggetto delle istruttorie svolte dall'Ufficio. Tali rischi derivano spesso dalla circostanza che nella maggior parte dei dossier sanitari esaminati gli stessi sono stati sviluppati in modo non strutturale e organizzato, bensì partendo da alcune iniziative estemporanee di informatizzazione delle cartelle cliniche di reparto o di ambulatorio e, quindi, senza tener conto del fatto che si andava predisponendo un sistema informativo in grado di gestire potenzialmente l'intera storia clinica di un individuo. Ciò ha determinato la realizzazione di sistemi in cui la mancanza di certezza sull'autenticità delle informazioni presenti, la possibilità che le stesse siano accessibili e modificabili da parte di soggetti non legittimati o siano persino diffuse, la non disponibilità delle stesse costituiscono rischi reali per lo più non considerati dalle strutture sanitarie almeno nelle prime fasi di realizzazione dei dossier.

Molti degli accertamenti ispettivi realizzati dall'Ufficio sono stati avviati, infatti, proprio a seguito di segnalazioni relative ad accessi abusivi ai dossier sanitari: consultazione, estrazione, copia delle informazioni sanitarie accessibili tramite il dossier da parte di personale amministrativo o personale medico che non era stato mai coinvolto nel processo di cura del paziente e che per motivi di interesse personale aveva acceduto allo stesso per poi divulgare le informazioni così acquisite a terzi all'insaputa dell'interessato. Nella maggior parte dei casi sottoposti all'attenzione dell'Autorità l'accesso aveva riguardato informazioni relative a prestazioni sanitarie particolarmente delicate in merito alle quali l'ordinamento vigente ha posto specifiche disposizioni a tutela della riservatezza e della dignità dei soggetti interessati (ad es.,affezioni da HIV, interruzione volontaria della gravidanza, parto in anonimato).

A fronte di tali rischi e della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, l'Autorità intende delineare nelle presenti Linee guida *un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte e conformare i trattamenti ai principi di legittimità stabiliti dal Codice, nel rispetto di elevati standard di sicurezza. Concreti strumenti di tutela che devono essere ricondotti al rispetto del diritto all'autodeterminazione informativa dell'interessato, delle misure atte a garantire l'esattezza, l'integrità e la disponibilità dei dati unitamente alla protezione da specifici rischi di accesso non autorizzato e di trattamento non consentito.*

2. L'INFORMATIVA AL *DOSSIER*

Il *dossier* sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica a vantaggio dei professionisti sanitari che presso lo stesso titolare del trattamento lo assistono, rappresenta un trattamento di dati personali specifico, volto 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.

TRATTAMENTO SPECIFICO E FACOLTATIVO

Il trattamento dei dati sanitari effettuato tramite il *dossier* costituisce, pertanto, un trattamento ulteriore rispetto a 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 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 e, quindi, da professionisti diversi, in occasione di altri eventi clinici occorsi in passato all'interessato che siano riferibili anche a patologie differenti rispetto all'evento clinico in relazione al quale l'interessato riceve la prestazione sanitaria.

Il trattamento dei dati personali effettuato mediante il *dossier* si differisce da 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 (*cfr., in particolare, l. 23.12.1978, n. 833;*

decreto del Ministro della sanità del 28.12.1991; Linee di guida del Ministero della Sanità del 17 giugno 199;, d.l. 9 febbraio 2012, n.5 convertito, con modificazioni, dalla l. 4 aprile 2012, n. 35, art. 47-bis, comma 1-bis citato).

In quanto tale 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.

DESCRIZIONE DEL *DOSSIER*

In particolare, nell'informativa al *dossier* deve 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.

L'interessato deve essere informato inoltre 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 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 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, doc. web n. 3619954).*

AMBITO DI CONOSCIBILITÀ

L'informativa al *dossier* è resa dal titolare del trattamento con riferimento al trattamento effettuato da parte dei professionisti e dei reparti o unità interne che prenderanno in cura l'interessato (*art. 79 del Codice*). Il titolare del trattamento deve, inoltre, 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 (*art. 79, comma 2, del Codice)*. Tali soggetti potranno, infatti, accedere esclusivamente ai *dossier* in relazione ai quali il titolare abbia già acquisito un consenso informato dei relativi interessati.

In alcuni dei sistemi informativi esaminati dal Garante è prevista una maschera all'interno dell'applicativo utilizzato per la gestione del *dossier* sanitario aziendale, consultabile da parte degli operatori sanitari, nella quale sono riportati gli estremi dell'acquisizione del consenso informato e delle altre manifestazioni di volontà dell'interessato in materia di protezione dei dati personali (ad es., quelle relative alla comunicazione a terzi di notizie relative allo stato di salute dell'interessato di cui all'art. 83, comma 2, lett. *f*) e *g*), del Codice).

L'interessato deve essere informato, infatti, 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 da parte di tutto il personale sanitario che fornirà nel tempo e a vario titolo assistenza sanitaria allo stesso.

Nell'informativa è necessario, inoltre, che sia specificata l'eventualità che il *dossier* sanitario sia consultabile anche da parte dei professionisti che agiscono in libera professione intramuraria -detta anche *intramoenia*- ovvero nell'erogazione di prestazioni al di fuori del normale orario di lavoro utilizzando le strutture ambulatoriali e diagnostiche della struttura sanitaria a fronte del pagamento da parte del paziente di una tariffa.

Al riguardo, si evidenzia che, nell'ambito dell'istruttoria delle segnalazioni ricevute, l'Ufficio ha riscontrato una forte preoccupazione degli

interessati in merito all'ampio ambito di accessibilità del *dossier* sanitario, costituendo questo un insieme di informazioni sensibili in grado di ricostruire in maniera significativa il profilo sanitario individuale. Ciò premesso, si ritiene opportuno che il titolare del trattamento, nell'indicare i soggetti che in qualità di responsabili o incaricati del trattamento possono accedere al *dossier* sanitario, illustri 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. In tal senso, l'informativa 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.

DIRITTI DELL'INTERESSATO

L'informativa deve indicare poi 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 (*cfr. successivo punto 5*).

DATI SOGGETTI A MAGGIOR TUTELA DELL'ANONIMATO

Una specifica menzione deve essere prevista nell'informativa 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).

CONOSCIBILITÀ DELL'INFORMATIVA

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 alcune realtà territoriali a tali proposte si sono affiancate attività di sensibilizzazione mediante spot pubblicitari o distribuzione di opuscoli informativi che illustrano le principali caratteristiche di tale trattamento di dati personali. Tali iniziative, secondo quanto sostenuto dai rappresentati delle strutture sanitarie che le hanno promosse, hanno contribuito a far meglio comprendere l'importanza di tale strumento e delle misure per la protezione dei dati personali con esso trattati ed hanno portato ad una sensibile riduzione della percentuale di dissensi al trattamento dei dati personali mediante il *dossier* da parte degli interessati.

PROFILI SANZIONATORI

Si evidenzia, infine, che in caso di omessa o inidonea informativa all'interessato è prevista una sanzione amministrativa (*art. 161 del Codice*).

3. IL CONSENSO AL *DOSSIER*

Come indicato nel precedente paragrafo il *dossier* sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo. All'interessato, infatti, deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un *dossier* sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento. Ciò significa che qualora l'interessato non manifesti il proprio consenso al trattamento dei dati personali mediante il *dossier* sanitario, il professionista che lo prende in cura avrà a disposizioni 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).

FACOLTATIVITÀ DEL CONSENSO

Ciò stante, l'eventuale mancato consenso al trattamento dei dati personali mediante il *dossier* sanitario non deve incidere negativamente sulla possibilità di accedere alle cure mediche richieste. Si rappresenta, al riguardo, che –sulla base degli elementi acquisiti da questa Autorità- nei progetti locali in cui la costituzione del *dossier* sanitario è stata accompagnata

da una campagna informativa attenta anche agli aspetti della protezione dei dati personali, la percentuale di negazione dei consensi al *dossier* è stata ben al di sotto del punto percentuale.

In tale quadro, 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)*.

Si rileva, pertanto, che ai fini dell'accesso al *dossier* da parte del personale sanitario non è necessario che venga acquisito volta per volta il consenso dell'interessato; il *dossier*, infatti, sarà accessibile nel tempo da parte di tutti gli operatori sanitari che lo prenderanno in cura sulla base del consenso che l'interessato avrà inizialmente prestato per il trattamento dei suoi dati personali mediante il *dossier*. Ciò stante, il professionista che a vario titolo (ad es., prestazione specialistica, nuovo ricovero, attività riabilitativa) interverrà nel processo di cura di un paziente che avrà già manifestato in passato il consenso al *dossier*, potrà accedere a tutti i dati ivi presenti.

REVOCA DEL CONSENSO

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 (*art. 22, comma 5, del Codice*), ma non devono essere più condivise con i professionisti degli altri reparti che prenderanno in seguito in cura l'interessato.

CONSENSO PER IL PREGRESSO

L'inserimento delle informazioni 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*.

Si evidenzia, inoltre, che i dati sanitari raccolti attraverso il *dossier* sanitario possono essere trattati, al pari di ogni altra informazione clinica, anche per fini di ricerca nel rispetto di quanto previsto dal Codice per tali tipi di trattamenti, ovvero, in via generale, previa acquisizione del consenso informato del paziente (*art. 110 del Codice*).

Si evidenzia che 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 (*artt. 13 e 82, comma 4, del Codice*).

CONSENSO DEL MINORE

Si evidenzia, infine, che il trattamento dei dati personali effettuato mediante il *dossier* sanitario in assenza del consenso informato dell'interessato non è lecito e, di conseguenza, i dati personali in tal modo trattati non possono essere utilizzati da parte del titolare *(artt. 11, comma 2, 13, 23 e 76 e ss. del Codice).* Il trattamento dei dati personali in violazione delle disposizioni sul consenso costituisce una fattispecie sanzionabile amministrativamente, rilevante anche in sede penale (*artt. 18, comma 4, 23, 26, 76, 81, 82, 162, comma 2-bis e 167 del Codice)*. Si precisa poi che, come anzidetto, la diffusione di dati personali è espressamente vietata dal Codice e, oltre a comportare l'applicazione della sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, può integrare la fattispecie di reato stabilita dall'art. 167, comma 2.

PROFILI SANZIONATORI

3.1. Particolari casi di consenso

Il titolare del trattamento deve acquisire una specifica manifestazione di volontà dell'interessato qualora nel *dossier* siano inserite 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. Si tratta, in particolare, dei dati soggetti a maggiore tutela dell'anonimato, ovvero relativi ad atti di violenza sessuale o di pedofilia, all'infezioni 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 (*l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269; l. 6 febbraio 2006, n. 38; l. 5 giugno 1990, n. 135; d.P.R. 9 ottobre 1990, n. 309; l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349; l. 29 luglio 1975, n. 405*). In tali casi, infatti, l'interessato può legittimamente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati (ad es., solo dallo specialista presso cui è in cura), fermo restando la possibilità che agli stessi possano sempre accedere i professionisti che li hanno elaborati.

Nel caso in cui il titolare intenda trattare anche tali dati personali mediante il *dossier* è pertanto necessario che acquisisca un autonomo e specifico consenso dell'interessato, che può essere raccolto unitamente a quello sul *dossier* o anche in occasione dell'erogazione della specifica prestazione sanitaria.

3.2. Prestazioni in emergenza

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.

Fatto salvo quanto previsto in via generale dall'art. 82 del Codice, ciò vale anche nel caso del paziente che giunga al pronto soccorso in gravi condizioni e non sia in grado di esplicitare alcuna specifica volontà.

Qualora l'interessato abbia acconsentito al trattamento dei suoi dati personali mediante il *dossier* sanitario, questo potrà essere consultato, nel rispetto dell'Autorizzazione generale del Garante, 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 - doc. web n. 3619954)* ad es., nei casi di rischio di insorgenza di patologie su soggetti terzi a causa della condivisione di ambienti con l'interessato.

4. I SISTEMI INFORMATIVI PER L'ORGANIZZAZIONE DEI SERVIZI TERRITORIALI DI ASSISTENZA PRIMARIA

Nel corso delle istruttorie avviate dall'Ufficio in merito ai trattamenti di dati personali effettuati mediante il *dossier* sanitario si è riscontrata l'implementazione di forme di integrazione di dati sanitari nell'ambito dell'organizzazione dei servizi territoriali di assistenza primaria previsti dall'art. 1 del d.l. 13 settembre 2012, n. 158, convertito in legge, con modificazioni, dall'art.1, comma 1, l. 8 novembre 2012, n. 189 (c.d. riforma Balduzzi). Secondo tale riforma, al fine di migliorare il livello di efficienza e di capacità di presa in carico dei cittadini, le regioni devono definire l'organizzazione dei servizi territoriali di assistenza primaria secondo modalità operative che prevedono forme organizzative monoprofessionali e multiprofessionali. Le prime, denominate "aggregazioni funzionali territoriali", condividono -in forma strutturata- obiettivi e percorsi assistenziali; le forme organizzative multiprofessionali, denominate "unità complesse di cure primarie", erogano prestazioni assistenziali tramite il coordinamento e l'integrazione di diversi soggetti quali i medici, le altre professionalità convenzionate con il Servizio Sanitario Nazionale e gli infermieri. Secondo quanto previsto dalla citata riforma, le forme multiprofessionali operano anche attraverso la costituzione di reti di poliambulatori territoriali in coordinamento e collegamento telematico con le strutture ospedaliere.

CONDIVISIONE DI SISTEMI INFORMATIVI

L'attuazione di tale riforma determina la nascita di sistemi informativi condivisi tra i diversi soggetti del Servizio Sanitario Nazionale indicati dalla stessa, in assenza -almeno allo stato- di una disciplina di attuazione che tenga conto dei connessi aspetti relativi alla protezione dei dati personali. Ciò stante, l'Autorità, nelle presenti *Linee guida*, ritiene necessario evidenziare ai diversi titolari del trattamento coinvolti la necessità di rispettare le misure e

gli adempimenti previsti dal Codice, nonché di operare attenendosi all'osservanza dei presupposti di legittimità individuati dalla predetta riforma.

Secondo l'impianto descritto nella citata riforma, infatti, più titolari del trattamento condividono le informazioni sanitarie di un paziente, al fine di offrire allo stesso servizi territoriali integrati di assistenza primaria. Tale assetto, pur non essendo riconducibile ad una ipotesi di *dossier* sanitario (in quanto sono coinvolti più titolari del trattamento), nonché a quella di Fse (per la ristrettezza dei soggetti coinvolti e per il perseguimento di sole finalità di cura e comunque connesse esclusivamente all'assistenza primaria) prevede una significativa integrazione di informazioni sanitarie attraverso l'utilizzo di sistemi di matrice regionale.

POSSIBILI INTERAZIONI CON IL DOSSIER SANITARIO

Come evidenziato, i trattamenti di dati personali descritti nella norma sopra ricordata sono effettuati da diversi e ben individuati titolari del trattamento che sono chiamati ad offrire servizi territoriali integrati di assistenza primaria. In relazione a tali attività, le regioni e gli stessi titolari devono porre attenzione in merito alla circostanza che tale realtà possa configurare una ipotesi di contitolarità del trattamento (*art. 4, comma 4, lett. f), del Codice*). In tale caso, a tutti i soggetti coinvolti competeranno le decisioni in ordine alle finalità e modalità del trattamento ivi comprese quelle relative al profilo della sicurezza.

MISURE A TUTELA DEI DATI TRATTATI

Nel rispetto del principio di liceità, il trattamento dei dati sanitari può essere posto in essere solo dai soggetti espressamente indicati dalla citata riforma e per le finalità di assistenza in essa individuate.

Tale trattamento, perseguendo finalità di cura dell'interessato, deve pertanto, essere effettuato solo previo consenso informato dello stesso. L'informativa, in particolare, deve rendere evidente l'ambito di operatività di tali sistemi, nonché indicare la sfera di conoscibilità dei dati all'interno dei

soggetti individuati dalla legge. Specifiche istruzioni devono essere fornite ai soggetti individuati dal decreto, che in qualità di responsabili o incaricati del trattamento, possono accedere a tali banche dati.

Con specifico riferimento al collegamento telematico con le strutture ospedaliere, 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 di necessità, pertinenza, non eccedenza e indispensabilità; le operazioni di accesso siano registrate in appositi file di *log* ai fini della verifica della liceità del trattamento dei dati; siano realizzate procedure per assicurare l'integrità, la disponibilità dei dati e il ripristino degli stessi in caso di guasti, malfunzionamenti o eventi disastrosi.

5. DIRITTI DELL'INTERESSATO

Il titolare del trattamento, ovvero la struttura sanitaria presso la quale è effettuato il trattamento dei dati personali mediante il *dossier* sanitario, deve garantire che l'interessato possa esercitare nei confronti di tale trattamento i diritti indicati nell'art. 7 del Codice. 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*).

Essendo il *dossier* sanitario 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.

LOGICA DEL TRATTAMENTO

In modo speculare rispetto a quanto previsto nell'informativa, 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 (cfr., paragrafo 1) (*art. 7, comma 2, lett. e), del Codice*).

AMBITO DI CONOSCIBILITÀ

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 (*Provvedimento generale del 24 luglio 2008 Linee guida per i trattamenti di dati*

ANNOTAZIONI

personali nell'ambito delle sperimentazioni cliniche di medicinali - doc. web n.1533155) (*art. 7, comma 3, lett. a), del Codice*).

5.1. 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 dati o documenti sanitari consultabili tramite tale strumento. Ciò in analogia a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di alcuni eventi sanitari che lo riguardano. Ciò, anche nel rispetto della legittima volontà dell'interessato di richiedere il parere di un altro specialista senza che quest'ultimo possa essere influenzato da quanto già espresso da un collega.

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. 9 dello schema di decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico; cfr. anche Linee guida nazionali sul Fascicolo sanitario elettronico adottate dal Ministero della salute l'11 novembre 2010).*

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, si evidenzia che di per sé il *dossier* sanitario costituisce uno strumento informativo incompleto. Indipendentemente dalle ipotesi di oscuramento, infatti, il *dossier* include solo le informazioni cliniche derivanti dagli accessi del paziente nella struttura sanitaria che utilizza il *dossier* e non

anche quelle relative agli accessi effettuati presso altre strutture pubbliche e private.

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.

OSCURAMENTO DELL'OSCURAMENTO

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").

Il titolare del trattamento è tenuto ad informare i soggetti abilitati ad accedere ai *dossier* in ordine alla possibilità che gli stessi possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento.

CONSEGUENZE DELL'OSCURAMENTO

Nel caso in cui l'interessato richieda l'oscuramento delle informazioni e/o dei documenti oggetto dello stesso, 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.

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.

Secondo quanto riportato dagli operatori di settore coinvolti nelle istruttorie avviate dall'Ufficio, laddove agli interessati sia stato ben illustrato sia l'esercizio di tale diritto che le implicazioni mediche di tale scelta -anche grazie all'intervento di personale sanitario qualificato- la percentuale di oscuramento -come quella di negazione del consenso al *dossier*- è risultata essere minore dell'1%.

5.2. Diritto alla visione degli accessi al *dossier*

Nella quasi totalità delle segnalazioni ricevute dal Garante circa il trattamento dei dati personali effettuato mediante il *dossier* sanitario sono stati lamentati accessi al *dossier* da parte di personale amministrativo o sanitario che non era stato mai coinvolto nel processo di cura dell'interessato. L'accesso, come indicato anche da alcune pronunce giudiziarie intervenute sui casi oggetto di segnalazioni, era stato posto in essere non per finalità di cura dell'interessato, bensì per acquisire informazioni sanitarie per scopi personali (es., curiosità, cause giudiziarie tra le parti) o commerciali. In tali casi il soggetto che aveva effettuato l'accesso poteva -con le proprie credenziali- accedere a tutti i *dossier* sanitari aziendali, indipendentemente dalla circostanza di essere intervenuto nel processo di cura dei soggetti a cui i *dossier* si riferiscono.

Tali realtà mettono in risalto i concreti rischi di accesso non autorizzato ai dati personali trattati mediante il *dossier* sanitario che possono essere ben limitati attraverso l'adozione di idonee misure di sicurezza e un'attenta individuazione dei profili e dei livelli di autenticazione e di accesso ai

sistemi. Nel contempo, tali rischi rendono necessario porre l'attenzione sulla necessità di riconoscere all'interessato di poter richiedere al titolare del trattamento quali siano stati gli accessi al proprio *dossier* sanitario. In tal senso, nel citato schema di decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico, su cui il Garante ha espresso il proprio parere in data 22 maggio 2014 (*doc. web n. 3230826*), 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.

RICHIESTA DELL'INTERESSATO

In tale quadro, si prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice che i titolari del trattamento forniscano all'interessato, che abbia manifestato il proprio consenso al trattamento dei dati personali mediante il *dossier* sanitario, un riscontro alla richiesta avanzata dallo stesso o da un suo delegato, volta 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 (*al riguardo, cfr. Parere sullo schema di provvedimento del Direttore dell'Agenzia dell'entrate per l'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati del 19 febbraio 2015, doc. web n. 3741076*). Di tale diritto esercitabile dagli interessati devono essere opportunamente informati anche i soggetti autorizzati ad accedere al *dossier* sanitario.

OBBLIGHI DEL TITOLARE

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.

6. ACCESSO AL DOSSIER

Come già rappresentato, 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 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 in tale processo di cura e deve essere posto in essere esclusivamente da parte dei soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale (ad es., visite per l'accertamento dell'idoneità lavorativa o per il rilascio di certificazioni necessarie al conferimento di permessi o abilitazioni) (*cfr., punto 5 delle citate Linee guida del 2009*).

PROFILO SOGGETTIVO

Al riguardo, è necessario evidenziare che l'insieme delle informazioni sanitarie trattate mediante il *dossier* sanitario costituisce una banca dati di significativo rilievo non solo clinico ma anche economico. E' facilmente intuibile, infatti, l'interesse economico che vari soggetti potrebbero vantare nei confronti di tale insieme di dati, la consultazione del quale rende agevolmente possibile ricostruire una significativa parte della storia clinica di un individuo. 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, è necessario, pertanto, che il titolare ponga 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 o nell'ambito delle procedure di un trapianto.

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. Il titolare del trattamento deve, pertanto, effettuare un monitoraggio delle ipotesi 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.

CASISTICA

L'Autorità ha riscontrato che in molte delle strutture sanitarie presso le quali sono stati effettuati accertamenti ispettivi tali cautele sono state tradotte mettendo automaticamente a disposizione del professionista sanitario i *dossier* dei pazienti 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). In tali realtà, i professionisti hanno, poi, la possibilità di consultare altri *dossier* sanitari motivando l'accesso sulla base di una casistica predeterminata dallo stesso titolare ed effettuata in base all'osservazione dei casi per i quali i professionisti generalmente accedono ai *dossier* (ad es., trapianti, richiesta di

consulenza, guardia medica, richiesta di chiarimenti terapeutici da parte dell'interessato). In alcune delle strutture oggetto di accertamento è stato concesso al professionista sanitario di accedere ai *dossier* sanitari anche in ipotesi diverse da quelle predeterminate dal titolare; in tali casi l'operatore aveva l'obbligo di documentare per iscritto la motivazione di tale accesso. Tali motivazioni venivano poi analizzate, al fine di valutare l'opportunità di introdurre nuove casistiche predeterminate in base alle quali consentire l'accesso al *dossier*.

PROFONDITÀ DELL'ACCESSO

Si evidenzia, inoltre, che compito del titolare del trattamento non è solo quello di individuare i soggetti che hanno diritto ad accedere ai *dossier* sanitari aziendali perché intervengono nel processo di cura dei pazienti, ma anche quello di individuare la c.d. "profondità dell'accesso". Il titolare deve valutare, infatti, 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. Ciò appare maggiormente evidente nelle ipotesi in cui sia consentito l'accesso al *dossier* a parte del personale che svolge funzioni amministrative correlate alla cura dell'interessato.

In molti dei sistemi di *dossier* oggetto di attenzione da parte dell'Ufficio è stato, infatti, riscontrato che tale strumento veniva utilizzato anche per svolgere delle funzioni amministrative strettamente connesse con il percorso di cura del paziente (ad es., 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). 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.

Il personale amministrativo operante all'interno della struttura sanitaria in cui viene utilizzato il *dossier* può, pertanto, in qualità di incaricato del

trattamento, consultare solo le informazioni indispensabili per assolvere alle funzioni amministrative cui è preposto (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche può consultare unicamente i soli dati indispensabili per la prenotazione stessa).

L'analisi circa la profondità degli accessi deve essere effettuata anche con riferimento al personale sanitario, al fine di valutare se sia sempre necessario consentire l'accesso a tutti i dati consultabili tramite il *dossier* da parte di tutti i soggetti abilitati (*artt. 11, comma 1, lett.* d) *e 22, comma 5, del Codice*).

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*.

FUNZIONI AMMINISTRATIVE

In alcune delle realtà sanitarie in cui l'Ufficio ha effettuato accertamenti ispettivi è emerso che il *dossier* sanitario viene utilizzato anche come strumento per acquisire i dati necessari per adempiere ai debiti informativi che la struttura sanitaria ha nei confronti delle regioni o di altri organi istituzionali nazionali (es., Ministero della salute). Al riguardo, giova evidenziare che i soggetti preposti all'assolvimento di tali obblighi devono avere accesso alle sole informazioni indispensabili ad assolvere agli stessi. Inoltre, si rappresenta che, 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.

Si precisa, infine, che eventuali richieste dell'Autorità giudiziaria con riferimento ai dati o ai documenti accessibili mediante il *dossier* devono essere soddisfatte nel rispetto dei limiti stabiliti dalla legge, ma non possono costituire una base legittimante la raccolta dei dati. Più precisamente, il titolare del trattamento potrà fornire, nei limiti di legge, all'Autorità giudiziaria le informazioni in suo possesso, non costituendo l'eventualità che in futuro si presentino tali istanze un'idonea fonte legittimante la raccolta di dati personali dell'interessato. Resta ovviamente ferma la normativa in materia di diritti di accesso ai documenti amministrativi *(l. 7 agosto 1990, n. 241 e successive modificazioni e integrazioni*).

6.1. Incaricati e responsabili

Tutti i soggetti abilitati a trattare i dati personali mediante il *dossier* sanitario devono essere designati incaricati o responsabili del trattamento (*artt. 4, comma 1, lett.* g) *e h), 29 e 30 del Codice*).

Le persone fisiche legittimate a consultare *dossier* devono essere adeguatamente edotte in merito alle modalità di utilizzazione di tali strumenti, nonché alle misure adottate per la tutela dei dati personali trattati mediante gli stessi.

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

ISTRUZIONI

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 siano fornite loro idonee istruzioni in merito al trattamento di dati personali effettuato mediante il *dossier* e alle connesse responsabilità.

PROFILI SANZIONATORI

Si precisa, infine, che la mancata designazione ad incaricati 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*).

7. SICUREZZA DEI DATI

Come già indicato dal Garante nelle citate *Linee guida* del 2009, la particolare delicatezza dei dati personali trattati mediante il *dossier* sanitario impone 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.*).

I RISCHI

Molti sono i rischi che il titolare del trattamento dei dati personali effettuato mediante il *dossier* sanitario deve valutare nella scelta delle misure di sicurezza da adottare al riguardo. Accesso abusivo, furto o smarrimento parziale o integrale dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi, comunicazione a soggetti non legittimati sono i principali rischi incombenti sui dati personali cui possono incorrere i titolari del trattamento nell'utilizzo di tali sistemi. Ai predetti pericoli si aggiunge la necessità di garantire la certezza circa l'origine del dato trattato, la sua esattezza, integrità e non modificabilità, nonché la disponibilità dello stesso; in merito a tali ultimi aspetti, oltre ai profili relativi alla protezione del dato personale, si aggiungono quelli attinenti alla responsabilità deontologica e professionale.

A tal fine, l'Autorità ritiene opportuno indicare le principali misure di sicurezza che il titolare del trattamento dei dati personali effettuato mediante il *dossier* sanitario deve adottare.

a) 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 e amministrativo. Le predette esigenze devono essere individuate 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 consentire, come sopra ricordato, un accesso selettivo al *dossier* sanitario fondato sul principio di indispensabilità del dato trattato. Attraverso questi 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. Soprattutto in tale ultimo, caso l'accesso deve essere consentito solo dopo aver individuato i dati strettamente indispensabili a cui tali soggetti devono avere accesso per l'espletamento delle funzione ad essi assegnate.

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.

b) Tracciabilità degli accessi e delle operazioni effettuate

Pur in assenza di disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni con riguardo sia all'*an* sia al *quantum*, e comunque ferma restando la disciplina in materia di controllo a distanza dell'attività dei lavoratori, le strutture sanitarie, nell'ambito della discrezionalità riconosciuta nell'organizzare la funzione di *compliance*, 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.

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.

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.

Alla luce dell'esperienza maturata in sede ispettiva, relativa all'enorme mole di accessi ai *dossier* sanitari che vengono effettuati all'interno delle strutture sanitarie giornalmente in modalità di sola consultazione, si ritiene congruo stabilire che i *log* delle operazioni siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.

c) 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*.

Il titolare deve prefigurare, quindi, 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).

In tal senso, la gestione dei dati personali effettuata attraverso il *dossier* sanitario deve essere oggetto di una periodica attività di controllo interno da

parte del titolare del trattamento, che consenta di verificare in concreto l'adeguatezza delle misure di sicurezza, sia di tipo organizzativo, sia di tipo tecnico, riguardanti i trattamenti dei dati personali, e la loro rispondenza alle disposizioni vigenti.

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.

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 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.

d) 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 (*artt. 22, comma 6 e 7 del Codice*). 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.

7.1. *Data breach*

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, anche in coerenza con le previsioni normative in tema di Fse, 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.

COMUNICAZIONE AL GARANTE

A questo fine, 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" al provvedimento del 4 giugno 2015 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.

COMUNICAZIONE ALL'INTERESSATO

In ragione della particolare delicatezza del trattamento dei dati effettuato mediante il *dossier* sanitario, l'Autorità ritiene, inoltre, 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, in termini generali, può consentire

all'interessato di minimizzare i rischi connessi alla violazione della disciplina di protezione dei dati personali.

7.2. *Data protection officer* (referente per la protezione dati)

In sintonia con quanto espresso nel parere sul citato schema di decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico, in ragione della particolare delicatezza delle informazioni trattate mediante il *dossier* sanitario, 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 casi di *data breach* precedentemente illustrati.