Cloud in Sanità: Vademecum essenziale sulla tutela dei dati personali

MANUALE SUI PRINCIPI, SULLE CARATTERISTICHE, SULLE SPECIFICHE NORMATIVE IN MATERIA DI PROTEZIONE DEI DATI DA APPLICARE IN ITALIA ALL'EROGAZIONE DI SERVIZI SANITARI CON TECNOLOGIA CLOUD COMPUTING

Autori: Avv. Luca Bolognini[1] – Avv. Enrico Pelino[2]

Nuova versione - 2016

---

[1] Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, avvocato del Foro di Roma, cofondatore dello Studio ICT Legal Consulting con sedi a Roma, Milano, Bologna e Amsterdam – l.bolognini@istitutoprivacy.it

[2] Fellow dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, avvocato del Foro di Bologna

1. INTRODUZIONE E CARATTERISTICHE DEL PRESENTE LAVORO

1 Il processo di migrazione in atto alla sanità elettronica

Il comma 1 dell'art. 47-bis del d.l. 9 febbraio 2012, n. 5, recante "*Disposizioni urgenti in materia di semplificazione e di sviluppo"*, convertito con modificazioni dalla L. 4 aprile 2012, n. 35 (*"Semplificazione in materia di sanità digitale"*) ha sancito la **preminenza della gestione elettronica** rispetto a quella tradizionale per quanto concerne le pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini, nei limiti di sostenibilità anche finanziaria per gli enti sanitari pubblici e privati interessati. Ha inoltre consentito, a partire dal 1° gennaio 2013, la conservazione **anche soltanto digitale** delle cartelle cliniche.

Si tratta di uno sviluppo che va visto come ulteriore, decisivo, spostamento in avanti nel processo di migrazione dei servizi sanitari a una gestione (prevalentemente o interamente) informatica.

2 Sintesi delle ragioni di questa migrazione

Le ragioni di opportunità connesse ad una gestione elettronica sono numerose:

- disponibilità di tutte le informazioni sanitarie con un click e in ogni momento (tendenzialmente 24 ore su 24 e 7 giorni su 7)
- accessibilità alle informazioni sanitarie da qualsiasi terminale abilitato
- completezza informativa
- standardizzazione dei formati
- abbattimento dei costi di archiviazione (*storage*) e dei volumi
- possibilità di verifica degli accessi alle informazioni sanitarie
- automatizzazione dei sistemi di prenotazione delle visite e ritiro dei referti, con abbattimento dei costi e risparmio di tempo per il cittadino
- semplificazione del *workflow* documentale in ambito clinico e amministrativo

Si tratta quindi di ragioni insieme di **maggiore efficienza** e di **risparmio di risorse**, che possono quindi essere allocate utilmente in altre direzioni.

Inoltre una gestione elettronica consente **prestazioni nuove** e difficilmente immaginabili con una gestione tradizionale, ad esempio la costituzione di un fascicolo sanitario elettronico (di seguito

"FSE"), popolato da informazioni sanitarie provenienti da una pluralità di strutture sanitarie, che registra ogni episodio clinico del paziente, dalla nascita alla morte.

3 Il cloud in ambito sanitario

Ulteriore fattore di risparmio è dato dall'adozione di tecnologie cloud, in quanto esse **abbattono i costi fissi** per l'acquisizione di strumenti informatici (hardware e software), come anche i costi di manutenzione e di aggiornamento, permettendo di convogliare la spesa soltanto sull'ottenimento del servizio desiderato e di farlo **in maniera flessibile** e **solo quando ce n'è bisogno**, in base alle reali esigenze di approvvigionamento. Ancora una volta, le risorse economiche liberate possono essere meglio indirizzate in direzioni diverse

Non a caso il ricorso a tecnologie cloud è indicato espressamente nel d.lgs. 7 marzo 2005, n. 82 (il Codice dell'amministrazione digitale, qui di seguito "CAD"), all'art. 68, co. 1, lett. d), quale **opzione da tenere presente** per la Pubblica amministrazione nella scelta dei servizi informatici.

Occorre pensare alla tecnologia cloud non solo per l'archiviazione o *storage* di dati sanitari, ma anche per la fruizione in cloud di potenti applicativi sanitari (ad esempio per la gestione del FSE) o per lo sviluppo dei medesimi su apposite piattaforme software in cloud.

In definitiva, il cloud può intervenire in ambito sanitario come:

- come modello IaaS (*Infrastructure as a Service*), ossia offrendo un servizio di infrastruttura, permettendo l'archivizione (*storage*) di dati sanitari;
- come modello SaaS (*Software as a Service*), ossia offrendo un servizio software, ad esempio attraverso la fruizione di appositi programmi applicativi;
- come modello PaaS (*Platform as a Service*), per lo sviluppo e l'hosting di loro applicazioni per la gestione dei dati sanitari.

Il servizio di *storage* può quindi essere variamente combinato con servizi applicativi.

4 Le norme e i principi

Nella migrazione alla sanità elettronica deve essere rispettata la disciplina applicabile ai medesimi servizi resi in via tradizionale. Occorre inoltre tenere conto delle disposizioni che si rendono applicabili per le specifiche caratteristiche del servizio elettronico (ad es. norme sul trasferimento dei dati sanitari extra UE, come disciplinato dal d.lgs. 30 giugno 2003, n. 196, più avanti "Codice privacy") e osservare la normativa che regola in modo specifico alcune attività di trattamento dei dati sanitari in un contesto informatico (ancora una volta il riferimento è al Codice privacy e al suo Allegato B). Bisogna, in questo senso, tenere presenti non solo i vantaggi connessi con l'ampia fruibilità del dato sanitario elettronico ma anche le correlate e peculiari vulnerabilità (criticità eventuali nel trasferimento dei dati personali extra UE, accessibilità ai dati, modificabilità, possibilità di perdita dei dati per eventi disastrosi, continuità operativa, ecc.)

Nell'analisi vanno anche tenute presenti linee guida elaborate con specifico riferimento al cloud in materia di servizi sanitari, come la Carta di Castelfranco.

Vi sono poi fonti più generali, in quanto non riferite espressamente al settore sanitario, che devono in ogni caso trovare applicazione. Si tratta delle norme contenute innanzitutto nel CAD, nel d.lgs. 12 aprile 2006 n. 163 (Codice dei contratti pubblici) e in altre fonti amministrative primarie. Occorre altresì tenere conto dei manuali elaborati da Digitpa/AGID, e delle linee guida, come quelle in materia di disaster recovery.

5 Il taglio, le caratteristiche e i contenuti del presente lavoro

Il presente lavoro si concentra soltanto sugli atti normativi che specificamente ineriscono al settore sanitario, considerando come elementi presupposti le fonti che più in generale regolano il settore amministrativo. Si farà soltanto un richiamo per punti ai principali aspetti da tenere presenti.

Occorre anche evidenziare che il taglio della presente analisi, senza rinunciare al rigore giuridico, sarà di di tipo manualistico-pratico, per privilegiare una fruizione più ampia dei contenuti.

L'obiettivo è quello di mettere a disposizione un **prontuario di veloce e semplice consultazione** che consenta un rapido orientamento (da completare con specifici approfondimenti successivi) anche da parte del non esperto, nella scelta delle soluzioni tecnologiche nella sanità elettronica.

In particolare, il lavoro ha la seguente struttura

- una prima parte con cenni alle caratteristiche essenziali nella scelta di un servizio cloud in ambito sanitario
- una seconda parte che indichi sinteticamente le norme da osservare in materia di protezione dei dati personali nella gestione e implementazione di servizi sanitari
- una terza parte dedicata specificamente (e senza pretesa di completezza, nella vasta offerta di strumenti di sanità elettronica) a una serie di servizi di ampia applicazione e sviluppo nel contesto della sanità elettronica, ossia, in ordine crescente di complessità, i seguenti:

- Referto online
- Archivio di referti online
- Cartella clinica online / Dossier sanitario elettronico (*electronic patient / medical record* o *EMR / EPR*)
- FSE *(electronic health record o EHR)*

PRIMA PARTE: CARATTERISTICHE ESSENZIALI NELLA SCELTA DI UN SERVIZIO CLOUD IN AMBITO SANITARIO

1 Fonti utilizzate

- Codice dell'amministrazione digitale [CAD]
- Garante privacy, Linee guida cloud [GarCloud]
- Carta di Castelfranco [Cast]
- WP29, opinione 5/2012 sul cloud computing [WP29_CLOUD]
- American Medical Association, *15 questions to ask before signing an EMR/EHR agreement* [AMA]

2 Caratteristiche da tenere presenti

Costi

- Costo complessivo del programma o soluzione. È decisivo rilevare che il costo **complessivo** deve tenere conto non solo del costo di acquisto, ma anche di quello di implementazione, di mantenimento e **supporto**. Sono inclusi in questa valutazione anche gli eventuali costi di assistenza 24/7, i costi di acquisto di licenze (per operatore sanitario / per struttura / in base ad altri criteri?) [CAD, art. 68, co. 1-bis, lett. a)] [AMA, n. 7]

Portabilità / interoperabilità

- Portabilità dei dati. Occorre privilegiare i servizi che favoriscono la portabilità dei dati, anche eventualmente tra fornitori di cloud diversi. Sul punto è necessario sia l'impegno contrattuale del fornitore di cloud di garantire, con procedura semplice, la portabilità di tutti i dati conferiti, rispettando l'architettura di cartelle e file, come anche le codifiche applicate ai dati (es. HL7), sia la scelta di un formato aperto (o, se proprietario, quantomeno pienamente e gratuitamente compatibile con formati aperti) per la portabilità. [CAD, art. 68, co. 1-bis, lett. b)] [GARCloud, pp. 13, 15] [Cast, n. 4]
- interoperabilità tra sistemi (collegato al punto precedente). [CAD, art. 68, co. 1-bis, lett. b)]

[GARCloud, pp. 13, 15] [Cast, n. 4]

- Adesione a standard internazionali (es. HL7, openEHR, EN 13606...[3]) per la codifica dei dati sanitari (collegato ai punti precedenti) secondo formati ampiamente adottati a livello internazionale e, come tali, di ampia e comune circolazione.

Strategie di selezione dei dati / strategie di localizzazione del cloud

- Selezionare i dati da inserire nel cloud. Il ricorso alla tecnologia cloud non deve necessariamente riguardare l'intero patrimonio informativo della PA. In particolare, ove il fornitore non assicuri sufficienti garanzie in relazione ai dati sanitari, genetici, biometrici, è opportuno valutare la possibilità di utilizzare di ricorrere al servizio di cloud computing solo per la gestione di alcuni settori di attività (es. applicativi per ufficio), con esclusione di altri. [GarCloud, p. 16]
- Private cloud o soluzione ibrida. Una soluzione collegata alla precedente è quella della scelta di un private cloud anziché di un public cloud per la gestione di alcune tipologie di dati particolarmente strategiche. Si può anche ipotizzare una **soluzione ibrida**, che integri un private cloud con un public cloud, per l'ottimizzazione della fornitura di servizio [Cast, n. 2]

Riuso (ove applicabile)

- Riuso dei programmi informatici realizzati su committenza delle Pubbliche amministrazioni. Questa ipotesi potrebbe applicarsi o no ai servizi cloud a seconda che gli applicativi utilizzati siano prodotti già sviluppati per il mercato oppure prodotti oggetto di specifica

---

[3]
- HL7 (Health Level 7): è uno standard riconosciuto a livello internazionale per definire struttura e semantica delle informazioni sanitarie in maniera da permettere lo scambio e la ricerca di dati informatici in ambito medico attraverso sistemi sanitari, elaborato dall'omonima organizzazione non-profit internazionale;

EN 13606: si tratta di uno standard europeo, basato sull'openEHR, dedicato allo scambio di informazioni tra sistemi EHR;

openEHR: si tratta di uno standard aperto per la gestione, lo *storage*, la ricerca di dati sanitari contenuti nei fascicoli sanitari elettronici (EHR), sviluppato dall'omonima fondazione internazionale. A differenza degli standard HL7 e EN 13606, l'openEHR non riguarda lo scambio di informazioni tra sistemi di EHR.

commessa da parte della Pubblica amministrazione e dunque realizzati per conto della PA, tenendo conto di particolari indicazioni della medesima. In quest'ultimo caso, la PA ha diritto ad avere il programma in **formato sorgente**, completo della documentazione disponibile, in **uso gratuito** ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni. [CAD, art. 68, co. 1]

- Portabilità dei programmi informatici da riutilizzare. Questa ipotesi trova applicazione nel caso in cui trovi applicazione la precedente. Occorre assicurare che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme e conformi alla definizione e regolamentazione effettuata da Digitpa/AGID [CAD, art. 69].
- Continuità operativa (CO). Occorre prendere in considerazione, in tema di continuità operativa, anche la scelta di mantenere comunque *in-house* una copia di quei dati (anche se non personali)[4] dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite, a meno che la soluzione cloud scelta non offra ampie assicurazioni su questo aspetto. [GarCloud, p. 15] [Cast, n. 6]
- Disaster recovery (DR). Vale quanto osservato al punto precedente. [GarCloud, p. 15] [Cast, n. 7]
- Certificazioni. Il possesso di certificazioni è criterio raccomandato dal cd. Gruppo ex art. 29 dei garanti europei[5] [WP29_CLOUD, p. 22]
- Compliance con le misure di sicurezza per assicurare il rispetto dei principi in materia di trattamento di dati personali (es. principio di finalità, affinché il fornitore non tratti i dati per scopi propri, es. data mining ecc.)

---

[4] Cfr. GarCloud, pp. 15-16: *"(...I)l titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (backup) dei dati allocati nella cloud, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità"*.

[5] WP29_CLOUD, p. 22: *"Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion... The adoption of privacy-specific standards and certifications is central to the establishment of a trustworthy relationship between cloud providers, controllers and data subjects."*.

Questioni giuridiche

- Giurisdizione. Si consiglia di prevedere espressamente la giurisdizione del giudice ordinario italiano, indicando anche il foro competente. [Cast, n. 5]
- Legge applicabile. Si consiglia di prevedere l'applicazione al contratto della legge italiana, specificando che ciò vale altresì per le misure di sicurezza alle quali deve attenersi il responsabile del trattamento [Cast, n. 5]
- PLA (Privacy Level Agreement). È preferibile specificare nel contratto dei **Privacy Level Agreement o PLA**. I PLA sono dei SLA (Service Level Agreement) che descrivono specificamente l'erogazione di servizi relativi ai dati personali. I PLA in sostanza indicano, attraverso una misura numerica (e come tale di immediata verifica), i livelli di erogazione del servizio che il fornitore cloud si impegna ad assicurare (ad es.: disponibilità dell'accesso dati sanitari 7 giorni su 7 sette, 24 ore su 24 nel 99,9% dei casi; tempo di latenza, ossia tempo necessario affinché una informazione sia restituita pari a X secondi; disponibilità 24/7 del servizio di assistenza nel 99,9% dei casi, ecc.). È opportuno che i PLA includano anche impegni specifici in materia di CO e DR. [CAD, art. 68, co. 1-bis, lett. c)]
- Formalizzazione della responsabilità del cloud provider. È opportuno disciplinare espressamente la responsabilità del cloud provider nel caso di inadempimento rispetto agli obblighi contrattuali [Cast, n. 9]
- affidabilità del fornitore. È opportuno valutare la **stabilità societaria del fornitore**, ciò perché gli impegni contrattuali, anche in materia di CO e DR, devono poter essere concretamente garantiti. Occorre inoltre tenere conto delle referenze, le garanzie offerte in ordine alla confidenzialità dei dati e alle misure adottate. [GARCloud, p. 14]
- eventuale ruolo di intermediario del fornitore cloud. Il fornitore cloud potrebbe a sua volta utilizzare servizi cloud (es. infrastrutturali) forniti da terzi. In tal caso i dati conferiti verrebbero fisicamente a trovarsi nei server di tali terzi soggetti e sarebbero pertanto potenzialmente esposti anche alla normativa applicabile nei paese o nei paesi in questione. [GarCloud, p. 16]

Norme e principi richiamati dall'applicazione del diritto italiano in tema di protezione dei dati personali

- (per il dettaglio si vedano la parte seconda e terza di questo lavoro, dedicate rispettivamente alle misure di sicurezza da osservare, specialmente in relazione al trasferimento di dati sanitari e genetici e alle caratteristiche specifiche di cui tenere conto nella gestione di strumenti specifici nell'offerta di sanità online)

PARTE SECONDA

MISURE DI SICUREZZA DA OSSERVARE - SOGGETTI SANITARI PUBBLICI

1 Fonti

- Codice privacy [CodPri]
- Allegato B al Codice Privacy [All_B]
- Garante, autorizzazione 8/2012 sui dati genetici [GarGen]
- Garante, *Linee guida sul referto online*, 25 giugno 2009 (doc. web n. 1630271) [GarRef]
- Garante privacy, Linee Guida DS [GarDS]
- Garante privacy, Linee Guida FSE / DSE [GarFSE]
- DPCM 29 settembre 2015, n. 178, art. 23
- WP29, *Working document on the processing of personal data relating to health in electronic health records (EHR)*, 15 febbraio 2007 [WP29_EHR]

È interessante notare che le ***Linee guida sul referto online*** rappresentano un utile campo di applicazione delle misure di sicurezza indicate nel Codice privacy a proposito dei dati sanitari, in quanto integrano queste ultime con opportune esemplificazioni concrete. Sembra a chi scrive che le indicazioni espresse nelle menzionate Linee guida possano del resto applicarsi, considerata l'equivalenza giuridica (il referto online è un documento informatico che contiene dati sanitari), più in generale a qualsiasi ipotesi di trattamento di dati sanitari su server remoti e/o connessi a Internet, fatte salve le specificità di forme particolarmente complesse di trattamento come il FSE (di cui si dirà più avanti) che prevedono, in aggiunta, ulteriori misure di sicurezza e cautele.

2 Trattamento di dati sanitari contenuti in elenchi, registri o banche di dati da parte della PA

Accesso e consultazione dei dati sanitari

I dati sanitari (e quelli sensibili più in generale) contenuti in elenchi, registri o banche di dati devono essere:

- trattati con tecniche di **cifratura** oppure [CodPri, art. 22, commi 6 e 7]
- resi temporaneamente inintelligibili (ad es., attraverso l'uso di codici identificativi), salva identificazione degli interessati in caso di necessità. [CodPri, art. 22, commi 6 e 7]

Modalità di trattamento

I dati sanitari devono essere:

- conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo (come ad esempio per i dati trattati a scopo amministrativo-contabile) [CodPri, art. 22, co. 7]. A tal fine si può operare la cifratura o la **separazione** della componente sanitaria del dato [All_B, n. 24]. La separazione può essere di natura fisica oppure logica [GarRef]

Circolazione dei dati sanitari

I dati sanitari:

- **non possono essere diffusi**, ossia essere resi disponibili a soggetti indeterminati [CodPri, art. 22, co. 8]
- possono invece essere comunicati a soggetti determinati o trasmessi (es., dal titolare al responsabile), ma il **trasferimento deve avvenire in forma cifrata** [All_B, n. 24]. In particolare, in caso di trasmissione dei dati tra *server* del titolare di trattamento e *client* dell'interessato, è stato specificato che essa deve avvenire *"attraverso protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – Secure Socket Layer)"*[6]. Si tratta peraltro di protocolli crittografici di uso comune in rete [GarRef]. Ugualmente, in GarRef, il Garante ha richiesto per la trasmissione di documenti allegati contenenti dati sanitari (referto online) l'utilizzo di password

---

[6] Occorre naturalmente seguire l'evoluzione tecnologica, per cui lo standard di riferimento odierno dovrebbe essere piuttosto considerato il TLS anziché l'SSL.

o di chiavi crittografiche per l'apertura del file

- nella trasmissione occorre evitare l'acquisizione non autorizzata del dato durante eventuale *caching*, a tal fine adottando tecniche idonee [GarRef]
- il destinatario della comunicazione dovrebbe essere individuato con sicurezza. A proposito del **destinatario persona fisica** è stato indicato *"l'utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication*[7]*"* [GarRef]. Va evidenziato sul punto che il ricorso a tecniche di *strong authentication* è indicato comunque come meramente preferenziale. Altra applicazione del principio dell'individuazione sicura dell'interessato è stata fatta in materia di invio di referto online via email al paziente, caso nel quale è stato richiesto quantomeno che si procedesse alla *"convalida degli indirizzi e-mail tramite apposita procedura di verifica on-line"*.

È opportuno in ogni caso rimarcare che, in ossequio al principio della minimizzazione dei trattamenti, tanto più rilevante in materia di dati sanitari, le operazioni di trattamento, anche quando lecite, non dovrebbero essere effettuate se non indispensabili, principio che si applica *a fortiori* alla circolazione dei dati.

Trasferimento dei dati sanitari extra UE

Il trasferimento dei dati sanitari all'interno della UE e dei paesi dello "Spazio economico europeo", o SEE, (Norvegia, Liechtenstein e Islanda) non richiede il rispetto di ulteriori requisiti, mentre nel caso di diverso paese di destinazione occorre comunque verificare che il livello di protezione dei dati personali sia **adeguato** a quello vigente in ambito UE. Attualmente questa condizione vale per un numero assai limitato di paesi: Andorra, Argentina, Australia, Canada, Guernsey, Isola di Man, Isole Faroe, Israele, Jersey, Nuova Zelanda, Principato di Monaco, Svizzera, Uruguay.

La valutazione in merito all'adeguatezza è effettuata dalla Commissione europea, basandosi anche sulle verifiche effettuate dal Gruppo di lavoro ex art. 29, ossia il gruppo dei garanti europei.

Nel caso non vi sia giudizio di adeguatezza, affinché il trasferimento sia consentito occorre invece fare riferimento a strumenti specifici:

---

[7] In vari provvedimenti, cfr. quello reperebile al doc. web n. 1482111, il Garante ha considerato tecniche di strong authentication quelle *"consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione"*. Una di queste tecnologie di autenticazione può essere quella biometrica.

1. ottenere il **consenso** dell'interessato. Si tratta dello strumento principale. Dovrà trattarsi comunque di un consenso specifico e ulteriore rispetto a quelli prestati dal paziente [CodPri, art. 43, co. 1, lett. a)]
2. applicare l'ipotesi di esonero prevista quando il trasferimento è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato [CodPri, art. 43, co. 1, lett. b)]
3. applicare l'ipotesi di esonero prevista quando il trasferimento extra UE *"è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21"* [CodPri, art. 43, co. 1, lett. c)]
4. utilizzare i *model contract/clause* elaborati dalla Commissione europea, vale a dire modelli contrattuali che vincolano il soggetto destinatario del trasferimento nel paese di arrivo dei dati personali [CodPri, art. 44, co. 1, lett. b)]
5. utilizzare le *binding corporate rule* (*BCR*), applicabili eventualmente all'organizzazione del responsabile del trattamento [CodPri, art. 44, co. 1, lett. a)]
6. utilizzare contratti *ad hoc* che vincolino il soggetto destinatario al rispetto dei principi vigenti nella UE in materia di trattamento dei dati personali, benché in questo caso sia necessaria comunque l'approvazione anche dell'autorità garante [CodPri, art. 44, co. 1, lett. a)]
7. utilizzare l'accordo sul *Privacy Shield* tra Commissione europea e Governo USA [CodPri, art. 44, co. 1, lett. b), accordo con decisione di adeguatezza della Commissione UE del 12 luglio 2016, sostitutivo del "Safe Harbor" e in vigore dall'1 agosto 2016[8]] (in caso di trasferimento dei dati a ulteriori sub-fornitori, di norma si usano altri strumenti, quali le *Model Clause*)

Cautelativamente, si consiglia in ogni caso di privilegiare soluzioni cloud che assicurino il trattamento dei dati sanitari **all'interno della UE / SEE**, ciò specialmente in relazione al FSE, come

---

[8] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

si dirà più avanti, o comunque l'adozione esplicita dei *model contract/clause* approvati dalla Commissione Europea.

Casi di esonero del consenso / consenso espresso da sostituti

Il trasferimento dei dati sanitari anche senza il consenso scritto dell'interessato e anche verso un paese che non offre un livello di protezione dei dati personali adeguato resta possibile in casi eccezionali, ai sensi dell'esonero di cui all'art. 43, co. 1, lett. d) Codice privacy quando è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se si tratta della salvaguardia o dell'incolumità fisica dell'interessato e questi non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Il consenso può anche intervenire successivamente nel caso di impossibilità di raccolta del consenso da tali soggetti sostituti o in caso di rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato (cfr. art. 82, co. 2 Codice privacy).

Un'applicazione software per la gestione di funzionalità relative al (o che comportano il) trasferimento di dati sanitari all'estero dovrebbe essere progettata tenendo in considerazione il livello certificato di adeguatezza del paese destinatario dei dati sanitari o, in mancanza, l'utilizzo dei già detti strumenti idonei a consentire comunque il trasferimento o infine l'avvenuta prestazione del consenso da parte dell'interessato (oppure la mancata prestazione per impossibilità, come da legge).

Trasferimento extra UE / SEE di dati sanitari pubblici e dei dati contenuti nel FSE / dossier sanitario

Quanto specificato sopra attiene ai profili generali in materia di esportabilità dei dati personali sanitari extra-UE/SEE. Vi possono essere, tuttavia, almeno due ambiti specifici che impongano ulteriori limiti alla circolazione internazionale dei dati sanitari.

Il primo caso è quello dei dati sanitari gestiti da soggetti pubblici (es. ASL, ospedali, ecc.). Il secondo caso riguarda i dati contenuti in FSE / DSE.

Con riferimento ai dati sanitari trattati e conservati da soggetti pubblici, deve ritenersi applicabile l'art. 9 comma 2 del DPCM 3 dicembre 2013, concernente le "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter , comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 [CAD]". Esso prevede, in particolare, che "*fatto salvo quanto previsto dal decreto legislativo 22 gennaio 2004, n. 42, in ordine alla tutela, da parte del Ministero dei beni e delle attività culturali e del turismo, sugli archivi e sui singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico,* ***i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale*** *e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle stabilite dal presente decreto.*"

Si tratta di una norma fortemente limitante, che tuttavia non va letta in senso di assoluto divieto al trasferimento all'estero di dati sanitari gestiti da soggetti pubblici: un'interpretazione eccessivamente restrittiva di tale norma secondaria, che perimetra al territorio italiano l'ambito di conservazione dei dati, implicherebbe, peraltro, *ipso facto*, la violazione del principio di libera circolazione dei dati personali intra-UE. Agli occhi dell'interprete, dunque, essa va intesa nel senso che vi debba sempre essere conservazione dei dati **anche** sul territorio nazionale, e non che sussista un qualsivoglia divieto generale di circolazione "operativa" di copie dei dati anche fuori dai confini nazionali.

Con riferimento al secondo caso, quello di FSE / DSE (per la definizione delle nozioni di FSE / dossier sanitario si rimanda alla parte terza di questo lavoro, comunque non si tratta di qualsiasi dato sanitario ma solo di quelli contenuti negli specifici strumenti FSE / DSE), è necessario notare come, nel provvedimento contenente le Linee guida in materia di FSE / dossier [GarFSE], il Garante abbia espressamente richiesto il consenso dell'interessato per il trasferimento dei dati sanitari. Vale la pena riportare il passaggio: *“Anche il* ***trasferimento*** *all'estero*[9] *dei dati sanitari documentati nel FSE/dossier per finalità di prevenzione, diagnosi e cura dell'interessato può avvenire* ***esclusivamente con il suo consenso****, salvo il caso in cui sia necessario per la salvaguardia della vita o della incolumità di un terzo (art. 43 del Codice)”.*

Identica posizione è espressa dal cd. Gruppo di lavoro ex art. 29, ossia la riunione dei garanti europei, che nel *working document* sul FSE del 15 febbraio 2007 hanno precisato che per tutti i trasferimenti di dati sanitari che interessano il FSE diretti fuori dall'aerea UE / SEE e comunque verso paesi che presentano livelli inadeguati di tutela dei dati personali:

- occorre il **consenso** degli interessati [WP29_EHR, p. 19]
- di regola sarebbe comunque opportuna la trasformazione **anonima** dei dati (ossia con dissociazione dell'elemento identificativo) o **pseudonima** [WP29_EHR, p. 19]

La prescrizione sembra derogare alle regole generali, in quanto pone effettivamente una limitazione rispetto alla ben più ampia ricchezza di ipotesi contemplate agli artt. 43 e 44 Codice privacy.

A ben guardare tuttavia la cautela espressa dai Garanti europei e da quello nazionale può essere ricondotta a sistema facendo riferimento ai principi generali sul trattamento dei dati personali, in particolare il principio di minimizzazione, di proporzionalità, di non eccessività del trattamento[10].

Va anche evidenziato che, nonostante l'indicazione di fare riferimento alla trasformazione anonima o pseudonima del dato sanitario in ambito FSE, viene anche espressamente suggerito dal gruppo dei garanti europei di:

- utilizzare servizi FSE (specialmente di *storage*) **localizzati in area UE / SEE** o comunque in paesi che rispettino un livello adeguato di protezione dei dati personali[11] [WP29_EHR, p. 19]

---

[9] Il riferimento all'“estero” deve intendersi qui come riferimento ai paesi extra-UE / SEE che non offrono un adeguato livello di protezione lascia perplessi.

[10] WP29_EHR, p. 19: *“Electronic availability of medical data in EHR systems can considerably enhance* diagnostic or *treatment facilities by making use of medical expertise available only in foreign medical institutions. Additional consultation of foreign experts for diagnostic purposes* ***usually does not require*** *revealing the identity of the patient. Therefore, if possible, such data should be transferred to countries outside the European Union/European Economic Area only in* ***anonymised*** *or at least* ***pseudonymised form****. If there is no explicit consent of the data subject for the transfer of personal data, this would also avoid the necessity of obtaining permission for this data transfer, as the data subject is not identifiable to the recipient”.*

[11] WP29_EHR, p. 19: “*Considering the* ***elevated risk*** *to the personal data in an EHR system in an environment without adequate protection, the Article 29 Working Party wants to underline that any processing – especially the* ***storage*** *– of EHR data* ***should take place within*** *jurisdictions applying the EU Data Protection Directive or an adequate data protection legal framework”.*

In ambito cloud si evidenzia pertanto la necessità di **appurare contrattualmente** quale sia la localizzazione geografica dei server utilizzati. Possono preferibilmente essere esplorate anche soluzioni di **tipo ibrido**, con costituzione di un cloud privato sito in Italia per gestione dei soli dati sanitari del FSE e trattamento della componente anagrafica su cloud pubblico in ambito UE / SEE o, con le opportune garanzie, in ambito anche extra UE / SEE.

La registrazione degli accessi al DS e il diritto di conoscere gli accessi da parte dell'interessato

Con le Linee Guida sul Dossier Sanitario [GarDS], il Garante ha prescritto alcuni obblighi e misure di sicurezza specificamente rilevanti per il Dossier Sanitario, e aggiuntivi rispetto a quelli già prescritti con le Linee guida su FSE / DSE [GarFSE]. Tra questi adempimenti di sicurezza, **la registrazione degli accessi al Dossier e il sistema di *audit logging*** sono probabilmente le più innovative. Giova citare in proposito le Linee guida GarDS:

"*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."

A tale misura si riconnette **il diritto per ciascun interessato i cui dati siano contenuti nel DS di richiedere evidenza degli accessi eseguiti al proprio dossier**. Recitano infatti le GarDS:

"[…] *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*".

Dati genetici

Gli strumenti di sanità elettronica potrebbero effettuare altresì trattamento di dati genetici, definiti come segue dall'autorizzazione 8/2012 (doc. web n. 2157564), n. 1), lett. a): *"dato genetico, il dato che, indipendentemente dalla tipologia, riguarda la costituzione genotipica di un individuo, ovvero* ***i caratteri genetici trasmissibili*** *nell'ambito di un gruppo di individui legati da vincoli di parentela".*

In aggiunta alle norme già viste in tema di **cifratura** o utilizzo di tecniche che assicurino la temporanea inintelligibilità del dato, e della **separazione** rispetto ai dati sanitari, è previsto il rispetto dei seguenti requisiti.

Raccolta e conservazione dei dati genetici

Il titolare è tenuto a:

- separare i dati identificativi del paziente **già al momento della raccolta** (salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato);
- nel caso di raccolta di dati genetici per l'esecuzione di test e di screening genetici[12], limitare la raccolta alle sole informazioni personali e familiari strettamente indispensabili all'esecuzione

---

[12] La definizione è data nell'autorizzazione, *cit.*, n. 1, lett. g): *"screening genetico, il test genetico effettuato su popolazioni o su gruppi definiti, comprese le analisi familiari finalizzate a identificare -mediante "screening a cascata"- le persone potenzialmente a rischio di sviluppare la malattia genetica, al fine di delinearne le caratteristiche genetiche comuni o di identificare precocemente soggetti affetti o portatori di patologie genetiche o di altre caratteristiche ereditarie".*

dell'analisi;

- nei trattamenti effettuati mediante test sulla variabilità individuale[13] non raccogliere dati sullo stato di salute o su altre caratteristiche degli interessati, ad eccezione del sesso.

Accesso ai dati genetici

- Strong authentication: Autenticazione con tecniche **biometriche**, in combinazione con informazioni note agli incaricati (es. credenziali d'autenticazione) [GarGen] [GarRef]

Trasferimento dei dati genetici

- cifratura con firma digitale conforme alla legge italiana, prima di trasferire i dati con posta elettronica certificata. É ammesso il ricorso a canali di comunicazione di tipo "web application" che prevedano protocolli di comunicazione sicuri e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione.

---

[13] Ugualmente, la definizione normativa è nell'autorizzazione, *cit.*, n. 1, lett. f): *"f) test sulla variabilità individuale, i test genetici che comprendono: il test di parentela volto alla definizione dei rapporti di parentela; il test ancestrale volto a stabilire i rapporti di una persona nei confronti di un antenato o di una determinata popolazione o quanto del suo genoma sia stato ereditato dagli antenati appartenenti a una particolare area geografica o gruppo etnico; il test di identificazione genetica volto a determinare la probabilità con la quale un campione o una traccia di DNA recuperato da un oggetto o altro materiale appartenga a una determinata persona".*

PARTE TERZA

ESAME DI ALCUNE SPECIFICHE AREE DELLA SANITÀ ELETTRONICA

Questa terza parte è dedicata alla trattazione di alcuni specifici settori di particolare interesse della sanità elettronica. L'ordine, come anticipato, è nel senso di una complessità e di un'integrazione crescente. Il primo strumento trattato, il referto online, oltre a fornire funzionalità specifiche e dirette al cittadino per la consultazione via Internet (questo è l'obiettivo essenziale dello strumento), può essere infatti integrato entro un più ampio sistema per la gestione di cartelle cliniche elettroniche / dossier sanitari elettronici, che al loro interno raccolgono appunto anche i referti online. A loro volta, cartelle cliniche elettroniche / dossier sanitari elettronici sono fonti di popolamento del più generale fascicolo sanitario elettronico.

REFERTI ONLINE

La refertazione online, intesa come messa a disposizione del referto al paziente tramite connessione Internet, è considerato uno strumento meramente aggiuntivo (e non sostitutivo) di quella tradizionale.

Vanno qui considerate alcune caratteristiche generali:

- firma digitale del medico. Il referto online deve essere firmato digitalmente dal medico che lo ha formato, parallelamente a quanto avviene con la sottoscrizione della sua versione cartacea. Tale requisito deve essere preso in considerazione nello studio di un sistema informatico di refertazione online.
- condizioni di liceità del trattamento. In ogni caso per essere attivato richiede:
    - **informativa** specifica
    - espressione di **consenso** autonomo da parte dell'interessato (sempre revocabile)
    - selettività del consenso. È importante sottolineare che si tratta di un consenso che può essere reso in ogni tempo **selettivo**: vale a dire che l'avere espresso consenso al servizio di refertazione online non preclude all'interessato di escludere dalla refertazione singoli

esami clinici

- due modalità di consultazione. La disponibilità all'interessato dei referti online è stata esaminata dal Garante secondo due forme:
  - consultazione da parte del paziente via web
  - invio del referto via posta elettronica al paziente

Consultazione tramite web

1. utilizzo di protocolli con standard crittografici e certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https tls/ssl);
2. evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;
3. autenticazione sicura dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
4. disponibilità limitata nel tempo del referto on-line (massimo 45 gg.);
5. controllo dell'interessato: facoltà di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.
6. Procedure di sicurezza che rendono immediatamente non disponibili per la consultazione on-line i referti relativi a un interessato che abbia comunicato la compromissione della sicurezza delle proprie credenziali di autenticazione

Spedizione del referto tramite posta elettronica

1. Spedizione del referto in forma di allegato a un messaggio e-mail e non come testo compreso nella body part del messaggio;
2. password o chiave crittografica per l'apertura del file rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B al Codice). Questa cautela può essere disapplicata su richiesta dell'interessato.
3. convalida degli indirizzi e-mail tramite apposita procedura di verifica online, in modo da evitare

la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

4. procedure di sicurezza che interrompono immediatamente l'invio per posta elettronica dei referti relativi a un interessato che abbia comunicato la compromissione della sicurezza delle proprie credenziali di autenticazione

Sms di mero avvertimento. L'eventuale utilizzo di un servizio di avviso tramite sms della disponibilità alla consultazione dei referti attraverso le modalità sopra descritte dovrebbe limitarsi a dare notizia della disponibilità del referto, senza indicazioni sul dettaglio della tipologia di accertamenti effettuati, del loro esito o sulle credenziali di autenticazione assegnate all'interessato.

Archiviazione dei referti

L'archiviazione dei referti online è assoggettata dal Garante espressamente alla stessa disciplina del dossier sanitario / FSE, si rimanda pertanto alle norme aggiuntive descritte più avanti in questo lavoro. In proposito si può comunque evidenziare fin da ora che l'archiviazione elettronica dei referti richiede una specifica informativa e un autonomo consenso.

È utile segnalare che una prima esperienza di refertazione online si è registrata già 2009 in seguito alla collaborazione tra il Gruppo Poste Italiane e l'Azienda ULSS9 di Treviso. Lo strumento è pensato come *"un vero e proprio archivio digitale personale per conservare, visualizzare e scaricare i referti medici online"* [14].

CARTELLA CLINICA ELETTRONICA (EMR / EPR)

Non si rinviene una definizione normativa di "cartella clinica". Tuttavia la definizione è data per implicita e la cartella clinica appare già dal 1938 oggetto di disciplina normativa[15]. Per una definizione operativa ci si può richiamare a quella fornita dall'allora Ministero della Sanità nel

---

[14] http://www.federsanita.it/html/notizie/it/treviso-parte-il-servizio-del-libretto-sanitario-elettronico.asp

[15] Ad esempio il Regio Decreto 30 settembre 1938 n. 1631, recante *"Norme generali per l'ordinamento dei servizi sanitari e del personale sanitario degli ospedali"*, prevede all'art. 24 che tra le attribuzioni del primario ci sia quella di curare sotto la propria responsabilità, *"la regolare tenuta delle cartelle cliniche e dei registri nosologici"*. Successivamente l'art. 7, co. 3 d.P.R. 27 marzo 1969, n. 128, recante *"Ordinamento interno dei servizi ospedalieri"*, ha previsto che *"il primario... è responsabile della regolare compilazione delle cartelle cliniche, dei registri nosologici e della loro conservazione, fino alla consegna all'archivio centrale"*. I riferimenti normativi successivi alla cartella clinica sono assai numerosi.

1992, che può essere usata come base di ragionamento: *“Insieme di documenti che registrano un* ***complesso eterogeneo*** *di informazioni sanitarie, anagrafiche, sociali, aventi lo scopo di rilevare il percorso diagnostico-terapeutico di un paziente al fine di predisporre gli opportuni interventi sanitari e di poter effettuare indagini statistiche, scientifiche e medico-legali. È uno strumento informativo individuale finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente”*[16]. Già da questa definizione traspare una **pluralità di finalità**, ossia non soltanto finalità di cura, ma anche di ricerca scientifica e statistica. Emerge inoltre la tendenza a non limitare la cartella clinica alla raccolta soltanto delle informazioni relative ad un singolo episodio clinico, dal momento del ricovero a quello della dimissione, con individuazione esatta del paziente, indicazione del motivo del ricovero, accertamenti diagnostici e specialistici, referti, terapie, ma a raccogliere, in senso più ampio, il complesso delle informazioni sanitarie disponibili in una struttura riferite anche a più episodi clinici di un determinato paziente, tendenza quest'ultima favorita dal ricorso alle tecnologie informatiche.

L'**evoluzione della cartella clinica** è in altre parole già nel senso di costituire un vero e proprio fascicolo sanitario elettronico che registri la storia di un determinato paziente all'interno di una struttura ospedaliera, detto anche **EMR** (*electronic medical record*) o anche **EPR** (*electronic patient record*)[17] ossia quello che il Garante designa anche come *dossier sanitario elettronico*. Va comunque notato che le definizioni registrano in questa materia confini fluttuanti.

È interessante notare che **non si rinvengono neanche criteri univoci** e di linee guida ufficiali sulle modalità di strutturazione e compilazione della cartella clinica, con la conseguente adozione di cartelle che differiscono notevolmente tra ospedali e anche tra le diverse unità operative di una stessa struttura sanitaria[18]. Questo comporta uno sforzo verso la standardizzazione anche in questo settore. Un tentativo in questo senso, con la creazione di un vero e proprio dossier sanitario del paziente è stato tentato attraverso un progetto recentemente promosso dal Ministero della Salute,

---

[16] La citazione è riportata in Ministero della Salute, *Sicurezza dei pazienti e gestione del rischio clinico - Manuale per la formazione dei Medici di Medicina Generale e dei Pediatri di Famiglia*, marzo 2010, p. 24, url http://www.salute.gov.it/imgs/C_17_pubblicazioni_1232_allegato.pdf

[17] EMR è espressione di derivazione soprattutto statunitense, EPR proviene dall'esperienza del Regno Unito. Sono considerate espressioni grosso modo equivalenti. Un richiamo sintetico alla definizione di EMR si trova per esempio in Ministero della Salute, *Mattone 9 – Realizzazione del patient file*, p. 7, url http://www.mattoni.salute.gov.it/mattoni/documenti/M9_Patient_File_CdR_11_07_07.pdf

[18] Così è espressamente rilevato nell'introduzione al programma per l'elaborazione di una Cartella Paziente Integrata (CPI), pubblicato sul Ministero della Salute, all'url: http://www.salute.gov.it/qualita/paginaDettaglioQualita.jsp?menu=programmi&lingua=italiano&id=1324

volto alla creazione della cosiddetta “Cartella Paziente Integrata” o CPI[19]. La CPI è ancora intesa come cartella clinica cartacea, tuttavia, per le sue caratteristiche di standardizzazione, si pone come passaggio di estrema utilità verso l'elaborazione di cartelle cliniche elettroniche che recepiscano, secondo criteri uniformi, esigenze espresse dagli operatori della sanità relativamente ai contenuti e alla struttura della cartella clinica[20].

Va evidenziato che il Garante nelle proprie Linee guida sul FSE (ved. più avanti), ha distinto concettualmente tra un *dossier sanitario del paziente*, inteso come complesso di dati sanitari relativi relativi a un paziente trattati all'interno di un'unica struttura sanitaria, e il *fascicolo sanitario elettronico*, nel quale convergono dossier elaborati da diverse strutture sanitarie e dunque rispetto al quale il singolo dossier sanitario rappresenta semplicemente una fonte di popolamento dei dati[21]. La cartella clinica elettronica va convergendo sempre più nel concetto di fascicolo sanitario elettronico, appare dunque artificioso nell'analisi mantenere una reale separazione tra i concetti.

Dal punto di vista della disciplina privacy adottata il Garante, tuttavia, formula le stesse prescrizioni per entrambi gli strumenti sanitari, ossia tanto per i dossier quanto per il FSE (che indubbiamente pongono le stesse questioni in materia di trattamento, benché su scala diversa), per le quali si rimanda al paragrafo successivo.

FSE (EHR)

Fonti principali

- d.l. 18 ottobre 2012 , n. 179, recante *“Ulteriori misure urgenti per la crescita del Paese”*, convertito con legge 17 dicembre 2012, n. 221, detto anche “decreto sviluppo bis”, art. 12

---

[19] Cfr. http://www.salute.gov.it/imgs/c_17_pubblicazioni_1679_allegato.pdf

[20] Cfr. Progetto CPI, cit. nota precedente, p. 6: “La cartella paziente integrata è stata inoltre pensata con una attenzione alla
fase successiva di digitalizzazione in cui la facilità d’interazione/comunicazione
con lo strumento, è alla base della qualità e sicurezza della pratica clinica”

[21] Si trova una distinzione tra *dossier sanitario* e FSE. Cfr. Garante privacy, Linee guida sul FSE, *cit.*: *“In particolare, si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata)al cui interno operino più professionisti. Si intende invece per FSE il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta). I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di FSE regionale”.*

[SvilBis]

- Ministero della Salute, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, Roma, 11 novembre 2010 [MinSal]
- Garante per la protezione dei dati personali, Linee guida FSE 16 luglio 2009, doc. web n. 1634116 [GarFSE]
- Codice privacy [CodPri]
- WP29, *Working document on the processing of personal data relating to health in electronic health records (EHR)*, 15 febbraio 2007 [WP29_EHR]
- Garante privacy, Linee Guida Dossier Sanitario 4 giugno 2015, doc. web. n. 4084632 [GarDS]
- D.P.C.M. 29 settembre 2015, n. 178/2015

Definizione

"Il fascicolo sanitario elettronico (FSE) e' l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito". Si tratta di una definizione normativa di cui all'art. 12, comma 1 del d.l. 18 ottobre 2012 , n. 179, recante *"Ulteriori misure urgenti per la crescita del Paese".* La stessa definizione era già presente nelle Linee guida 2010 sul FSE emanate dal Ministero della salute (cfr. pag. 6).

Il FSE è pensato come uno strumento commisurato all'**intera vita del paziente** e ad alimentazione continua nel tempo[22].

Finalità del FSE

Le finalità del FSE sono di **tre tipi**:

a) prevenzione, diagnosi, cura e riabilitazione [SvilBis, art. 12, co. 2]

b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico [SvilBis, art. 12, co. 2]

c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria [SvilBis, art. 12, co. 2]

L'indicazione delle finalità, diverse tra loro alle quali può assolvere il FSE ha una conseguenza sulla

---

[22] Cfr. Ministero salute, *Linee guida FSE 2010*, p. 7.

disciplina da osservare in materia di trattamento dei dati personali.

Finalità di prevenzione, diagnosi, cura e riabilitazione

Questa finalità (più sinteticamente "finalità di cura") è disciplinata dall'art. 76 Codice privacy. Per effetto di tale disposizione normativa, è necessario per il trattamento dei dati:

- informativa specifica per il FSE [GarFSE, GarDS]
- **consenso** al FSE (anche orale e annotato dall'operatore sanitario) [GarFSE]

Non è invece necessaria alcuna autorizzazione da parte del Garante (è necessario tuttavia il rispetto dell'autorizzazione sui dati genetici quando si tratta questo tipo di dati, cfr. parte seconda del presente lavoro)[23].

L'informativa per il FSE deve essere specifica e quindi chiarire gli elementi essenziali del trattamento attraverso FSE, così come il complesso dei diritti che ineriscono al paziente (es. diritto di oscurare alcuni dati sanitari)[24]. Il Garante ha chiarito che il consenso in questione costituisce **un consenso ulteriore e specifico** (consenso al FSE) che si aggiunge a quello prestato per le singole attività di prevenzione, diagnosi, cura e riabilitazione che confluiscono nel FSE. Nulla esclude che il consenso specifico al FSE sia manifestato già unitamente a quello per le singole prestazioni sanitarie, ai sensi dell'art. 81 Codice privacy[25]. Il riferimento all'art. 81, operato espressamente dall'Autorità garante, permette anche di concludere che il consenso al FSE può essere anche

---

[23] Garante privacy, *Linee guida sul FSE*.

[24] Le linee guida ministeriali sul FSE precisano alcuni elementi essenziali che devono essere contenuti nell'informativa (cfr. p. 18): *"l'informativa:*
□ deve spiegare in modo semplice le opportunità che offre tale strumento avanzato e innovativo per migliorare le procedure atte a garantire il diritto alla salute, ma, al tempo stesso, l'ampia sfera conoscitiva che esso può avere;
□ deve informare l'assistito che un suo diniego non ha alcuna conseguenza sul suo diritto alla prestazione di cura richiesta;
□ deve dare sufficienti indicazioni sulle modalità di funzionamento del nuovo strumento digitale;
□ deve indicare i soggetti che, nel prendere in cura l'assistito, possono accedere al FSE, nonché la connessa possibilità di acconsentire che solo alcuni di questi soggetti possano consultarlo;
□ deve informare l'assistito anche della circostanza che il Fascicolo potrebbe essere consultato, anche senza il suo consenso, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività (art 76 del decreto legislativo del 30 giugno 2003, n. 196);
□ deve evidenziare la circostanza che il consenso alla consultazione del Fascicolo da parte di un determinato soggetto (ad es., del medico di medicina generale o del medico di reparto in cui è avvenuto il ricovero) può essere riferito anche al suo sostituto;
□ deve fornire all'assistito gli estremi identificativi del/dei titolare/i del trattamento dei dati personali trattati mediante il FSE;
□ deve informare l'assistito che può esercitare in ogni momento i diritti di cui all'art. 7 e s. del Codice...".

[25] Cfr. Garante privacy, *Linee guida FSE*: *"Il consenso,anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (cfr. art. 81 del Codice), deve essere autonomo e specifico"*.

manifestato **oralmente** dal paziente e **annotato** dall'esercente la professione sanitaria e dall'organismo sanitario pubblico. La stessa disciplina è applicabile anche al dossier sanitario del paziente.

Il trattamento per finalità di cura è svolto, come precisa il comma 4 dell'art. 13 d.l. 179/12, da soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali che prendono in cura l'assistito[26]. È evidentemente escluso ogni altro soggetto, sia pure medico, che tratti il dato per finalità diverse dalla finalità di cura[27]. Di tali elementi si deve tenere conto **in fase di progettazione dell'eventuale software** di gestione del FSE, in maniera che l'accesso al FSE sia consentito non semplicemente a operatori sanitari, ma soltanto a operatori sanitari autorizzati.

Naturalmente, l'accesso per finalità amministrative al FSE è consentito senza queste limitazioni, ma (come si indicherà oltre) si tratta di un accesso effettuato previa dissociazione della componente identificativa dai dati personali, e dunque precludendo a chi accede l'individuazione del soggetto a cui i dati si riferiscono.

Triplice livello di consenso

Come si è detto, il Garante ha precisato che all'interessato va riconosciuto un ampio diritto di controllo sui dati sanitari inclusi nel FSE. L'interessato ha quindi diritto di stabilire, con ulteriore manifestazione di consenso, quali soggetti possano consultare i suoi dati sanitari contenuti nel FSE[28]. Ciò è stato recentemente ribadito per espressa disposizione normativa al comma 5 del d.l.

---

[26] Le citate Linee guida ministeriali del 2010 ricostruiscono alcuni scenari di utilizzo del FSE per finalità di cura. Si tratta delle seguenti (cfr. pp. 7-8):
“ il supporto a scenari e processi di cura: in quanto rende disponibile la storia clinica del paziente a tutti gli attori coinvolti;
* il supporto all’emergenza/urgenza in quanto permette ad un operatore sanitario di inquadrare un paziente a lui sconosciuto durante il contatto in emergenza/urgenza;*
* il supporto per la continuità delle cure: in quanto permette a diversi operatori che hanno già in carico un paziente di essere consapevoli delle iniziative diagnostiche e terapeutiche portate avanti dai colleghi;*
* il supporto alle attività gestionali ed amministrative correlate ai processi di cura: in quanto permette di condividere tra gli operatori le informazioni amministrative (es. prenotazioni di visite specialistiche, ricette, etc.) od organizzative/ausiliarie per le reti di supporto ai pazienti nelle cronicità e/o nella riabilitazione.”.*

[27] Cfr. Garante privacy, *Linee guida FSE cit.*: Sono dunque esclusi *“periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche e organismi amministrativi anche operanti in ambito sanitario. Analogamente, l'accesso è precluso anche al personale medico nell'esercizio di attività medico-legale (es. visite per l'accertamento dell'idoneità lavorativa o alla guida), in quanto, sebbene figure professionali di tipo sanitario, tali professionisti svolgono la loro attività professionale nell'ambito dell'accertamento di idoneità o status, e non anche all'interno di un processo di cura dell'interessato”.*

[28] Garante privacy, *Linee guida cit.*:*“...Devono essere previsti momenti distinti nei quali l'interessato possa esprimere la propria volontà, attraverso un consenso di carattere generale per la costituzione del FSE e di consensi specifici*

179/12, che ha naturalmente richiamato in tale contesto anche l'obbligo al segreto professionale per il personale medico che ha accesso ai dati trattati nel FSE. Il consenso specifico alla consultazione del FSE si riferisce ad informazioni non prodotte direttamente dall'operatore sanitario che procedere alla consultazione ma da altri operatori (l'operatore che le ha generate può comunque accedervi).

In definitiva, si riscontrano tre livelli di consenso:

1. consenso relativo alla <u>singola prestazione</u> sanitaria che alimenterà il FSE [GarFSE]
2. consenso specifico alla <u>costituzione</u> del FSE [GarFSE]
3. consenso specifico alla <u>consultazione</u> del FSE da parte di determinati operatori sanitari [GarFSE]

Il consenso al FSE, come sempre qualsiasi manifestazione di consenso ai sensi della normativa sulla protezione dei dati personali, è assolutamente **libero**, ossia non collegato, in caso di rifiuto, a conseguenze pregiudizievoli per l'interessato. Il principio generale della libertà del consenso è ribadito ulteriormente al comma 5 del d.l. 179/12 che dispone che il *“mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria”*. Sempre ai sensi della disposizione in esame, si deroga invece al consenso (ma anche in questo caso si applicano le regole generali, cfr. art. 24, co. 1, lett. e) e 82, co. 2 Codice privacy) nel caso di emergenza sanitaria.

<u>Revoca del consenso al FSE</u>

L'interessato può in ogni momento revocare il proprio consenso al trattamento mediante FSE. Con la revoca del consenso, non sarà più possibile a soggetti **diversi** da coloro che hanno generato i dati sanitari accedere a questi ultimi, mentre sarà sempre garantito l'accesso ai documenti sanitari da parte dei soggetti che li hanno redatti (es. informazioni relative a un ricovero utilizzabili dalla struttura di degenza)[29]. Ciò che verrà meno sarà quindi **la condivisione** tra operatori della sanità dei dati del paziente, che è la caratteristica essenziale del FSE.

<u>Residue finalità: ricerca scientifica e programmazione sanitaria</u>

---

ai fini della sua consultazione o meno da parte dei singoli titolari del trattamento (es. medico di medicina generale, pediatra di libera scelta, farmacista, medico ospedaliero)”.

Inoltre, *ibidem*: *“L'accesso deve essere permesso... agli altri soggetti che abbiano in cura l'interessato, sempre che quest'ultimo ne abbia autorizzato l'accesso... In alcuni progetti di FSE esaminati, l'accesso da parte di alcune categorie di soggetti (es. medici specialisti) è ad esempio autorizzato di volta in volta dallo stesso interessato attraverso la consegna di una smart card”*.

[29] Così Garante privacy, *Linee guida cit.*.

La finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico di cui alla lett. b) è riconducibile all'art. 110 Codice. Come tale, non si richiede il consenso dell'interessato per tale trattamento, nel rispetto di tutti gli elementi di cui alla norma citata[30].

Ugualmente, non è richiesto il consenso dell'interessato per finalità programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria (sopra sub lett. c)). Tale finalità è qualificata finalità di rilevante interesse pubblico ai sensi dell'art. 85, co. 1, lett. a) e b) Codice. verificare se è necessario regolamento o se i tipi di dati e le operazioni sono effettivamente descritti da legge o regolamento

Come chiarito dal comma 6 dell'art. 12 del d.l. 179/12, le finalità di ricerca scientifica (lett. b)) e quelle amministrative (lett. c)) sono realizzate dalle regioni e dalle province autonome, dal Ministero del lavoro e delle politiche sociali e dal Ministero della salute nei limiti delle rispettive competenze attribuite dalla legge.

In definitiva, quindi, ai sensi del Codice privacy, il consenso dell'interessato è necessario solo per la costituzione del FSE per finalità di cura, mentre **non è richiesto nessun ulteriore consenso nel caso di utilizzo del FSE per finalità di studio e ricerca scientifica né per lo svolgimento delle attività amministrative** correlate alla gestione del FSE.

Con riferimento alle modalità di strutturazione di applicazioni software per la gestione del FSE, si evidenzia, anche al fine della progettazione del servizio software per la gestione del FSE, che le finalità sopra individuate alle lettere b) e c) sono perseguite nel rispetto di modalità volte alla **dissociazione** dell'elemento identificativo dell'interessato dai dati sanitari che lo riguardano (cfr. comma 6 dell'art 12 del d.l. 179/12). Va poi tenuto presente in un'ottica di approccio ***privacy by design***, il principio di minimizzazione dei dati personali di cui all'art. 3 Codice, come anche i principi generali di cui all'art. 11 Codice. Il richiamo a tali norme è del resto fatto espressamente al comma 6, art. 12 del d.l. 179/12 in commento che impone che le predette finalità siano appunto realizzate *"senza l'utilizzo dei dati identificativi degli assistiti e dei documenti clinici presenti nel*

---

[30] Art. 110, co. 1, Codice privacy: *"Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40".*

FSE, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti, con il decreto di cui al comma 7, in conformità ai principi di proporzionalita', necessita' e indispensabilita' nel trattamento dei dati personali".

Il 29 settembre del 2015 è stato, finalmente, emanato il Regolamento (DPCM n. 178/2015), il quale all'art. 23 prevede quanto segue, imponendo, fra le altre misure, anche la notificazione delle violazioni di dati (*data breaches notification*, ved. comma 9) con riferimento ai dati contenuti nel FSE:

Art. 23
Misure di sicurezza e sistema di conservazione

1. Le operazioni sui dati personali, necessarie per l'adempimento alle disposizioni di cui al presente decreto, sono effettuate mediante strumenti elettronici con modalita' e soluzioni necessarie per assicurare confidenzialita', integrita' e disponibilita' dei dati, adottate in coerenza con le misure di sicurezza espressamente previste nel decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, e nel relativo disciplinare tecnico di cui all'Allegato B.
2. Ferme restando le misure di sicurezza di cui al Codice in materia di protezione dei dati personali, l'accesso al FSE e' consentito, per tutte le finalita' di cui al comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, esclusivamente utilizzando le modalita' di accesso e gli strumenti di cui all'articolo 64 del CAD.
3. La riservatezza dei dati trattati nell'ambito del FSE, ai sensi del Codice in materia di protezione dei dati personali ed, in particolare, dell'articolo 34, comma 1, lettera h), e' garantita dalle procedure di sicurezza relative al software e ai servizi telematici utilizzati, attuate in conformita' alle previsioni del CAD.
4. Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati devono essere attuati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi.
5. Per la consultazione in sicurezza dei dati contenuti nel FSE sono assicurati:
a) idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento;
b) procedure per la verifica periodica della qualita' e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
c) protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti;
d) individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
e) tracciabilita' degli accessi e delle operazioni effettuate;
f) sistemi di audit log per il controllo degli accessi e per il rilevamento di eventuali anomalie;

g) procedure di anonimizzazione degli elementi identificativi diretti, come definito dai decreti attuativi di cui all'articolo 35 del decreto legislativo 23 giugno 2011, n. 118, per il perseguimento delle finalita' di cui ai punti b) e c) del comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, fermo restando quanto previsto dall'articolo 15, comma 25-bis, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135.
6. La struttura e l'organizzazione dei dati contenuti nel FSE deve garantire, oltre alla corretta e differenziata articolazione dei profili per quanto concerne la classificazione delle tipologie di informazioni sanitarie indispensabili in relazione alle finalita' per cui vengono trattate, anche quella relativa ai diversi livelli autorizzativi dei soggetti abilitati all'accesso.
7. Le disposizioni di cui al comma 5 vengono attuate ai sensi delle specificazioni contenute nel disciplinare tecnico.
8. Ai fini di garantire il corretto impiego del FSE da parte degli utilizzatori e per renderli edotti dei rischi che incombono sui dati, nonche' delle misure di sicurezza adottate, vengono organizzate apposite sessioni di formazione, anche con riferimento agli aspetti di protezione dei dati personali, con particolare riferimento, all'accessibilita' delle informazioni, alle operazioni di trattamento eseguibili e alla sicurezza dei dati.
9. Nel caso in cui dati trattati nell'ambito del FSE subiscano violazioni tali da comportare la perdita, la distruzione o la diffusione indebita di dati personali, il titolare del trattamento effettua una segnalazione al Garante per la protezione dei dati personali, entro una settimana dal verificarsi dell'evento, contenente:
a) una descrizione della natura della violazione dei dati personali occorsa, compresi le categorie e il numero di interessati coinvolti;
b) l'indicazione dell'identita' e delle coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere piu' informazioni;
c) la descrizione delle conseguenze della violazione dei dati personali subita;
d) le misure proposte o adottate dal responsabile del trattamento per porre rimedio alla violazione dei dati personali.
10. La continuita' delle operazioni indispensabili per il servizio e il ritorno alla normale operativita' sono assicurate dall'adozione del piano di continuita' operativa e del piano di disaster recovery, di cui all'articolo 50-bis del CAD [articolo abrogato, nda].
11. Al FSE e ai documenti di cui all'articolo 2, comma 2, si applicano le disposizioni degli articoli 43 e 44 del CAD.
12. Le disposizioni di cui al comma 1 si applicano anche ai documenti di cui all'articolo 2, comma 3, adottati nell'ambito della singola regione o provincia autonoma.
13. Le disposizioni di cui al comma 1 non si applicano al taccuino dell'assistito, di cui all'articolo 4.

I diritti dell'interessato

Ai sensi dell'art. 7 Codice privacy, l'interessato ha diritto di conoscere l'origine dei dati trattati, la logica e la finalità del trattamento (inclusa la finalità amministrativa e l'eventuale finalità di ricerca scientifica), la modalità del trattamento, i soggetti a cui i dati sono comunicati, l'identificazione del titolare del trattamento e del rappresentante o dei rappresentanti (eventualmente quindi anche i fornitori di cloud o di altri servizi elettronici che siano inquadrati nel ruolo di fornitori).

Oscuramento selettivo di dati sanitari

L'interessato ha inoltre la possibilità di “**oscurare**” alcuni dati sanitari, ossia decidere (anche evidentemente in via preventiva) che non compaiano nel FSE. Può trattarsi ad esempio dell'esito di una singola visita specialistica o dell'assunzione di un farmaco[31]. Il sistema software di gestione del FSE deve pertanto essere strutturato in maniera tale da consentire questo livello di decisione da parte dell'interessato, la cui scelta può sempre essere reversibile (per cui l'interessato deve poter vedere, lui solo, l'intero contenuto del FSE e decidere a quali soggetti concedere i privilegi informatici per visualizzare determinate informazioni. L'oscuramento perciò dovrebbe poter essere selettivo). L'interessato può decidere in definitiva *“se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo”* (art. 12, co. 3-bis d.l. 179/12).

È altresì prevista la possibilità di non rendere neppure conoscibile (anche solo ad alcuni soggetti) la scelta dell'interessato di oscurare alcune informazioni. Il Garante sul punto ha parlato di “**oscuramento dell'oscuramento**”[32]. Anche questa forma di privacy (eventualmente limitata solo ad alcuni dei soggetti che possono accedere al FSE) deve essere considerata quando si sviluppa un'applicazione informatica per la gestione del FSE.

Il Garante ha comunque evidenziato che *“l'accesso al FSE/dossier deve essere sempre consentito al soggetto che ha redatto il documento con riferimento all'interessato medesimo”*, dal che sembra evincersi che l'oscuramento (come anche l'oscuramento dell'oscuramento) non possa operare nei confronti del personale sanitario che alimenta il FSE, limitatamente ai documenti apportati in via diretta.

---

[31] Ciò è espressamente previsto dal Garante privacy nelle già citate Linee guida sul FSE.

[32] Garante privacy, *ibidem*: *“L'"oscuramento" dell'evento clinico (revocabile nel tempo) deve peraltro avvenire con modalità tali da garantire che, almeno in prima battuta,tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento"). In tale quadro, alcuni progetti di Fse esaminati garantiscono l'esercizio della "facoltà di oscuramento" mediante una "busta elettronica sigillata" non visibile, apribile di volta in volta solo con la collaborazione dell'interessato, ovvero utilizzando codici casuali relativi a singoli eventi che non consentono di collegare tra loro alcune informazioni contrassegnate. Resta fermala possibilità per il titolare del trattamento di informare i soggetti abilitati ad accedere a tali strumenti che tutti i fascicoli o i dossier cui hanno accesso possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento. Nulla osta, inoltre, che il titolare del trattamento possa prevedere che l'interessato eserciti tale facoltà in presenza del medico che ha eseguito la prestazione sanitaria, affinché quest'ultimo gli possa illustrare le conseguenze, da un punto di vista clinico, di tale scelta”.*

Logica modulare nell'architettura del FSE

Inoltre, anche nell'organizzazione delle procedure di condivisione delle informazioni sanitarie, il Garante[33] ritiene necessario privilegiare le soluzioni che consentano una **distribuzione modulare** degli accessi in consultazione, in modo da non porre sullo stesso livello tutti i soggetti astrattamente autorizzati all'accesso e *"da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili. In alcuni progetti di FSE esaminati tale organizzazione modulare permette, ad esempio, di selezionare le informazioni sanitarie accessibili ai diversi titolari abilitati in funzione del loro settore di specializzazione (es. rete oncologica composta da unità operative specializzate nella lotta ai tumori), garantendo così l'accesso alle sole informazioni* ***correlate con la patologia in cura****. Analogamente, alcune categorie di soggetti quali i farmacisti, che svolgono la propria attività in uno specifico segmento del percorso di cura, possono accedere al FSE/dossier, ma limitatamente ai soli dati (o moduli di dati) indispensabili all'erogazione di farmaci (es. accesso limitato all'elenco dei farmaci già prescritti, al fine di valutare eventuali incompatibilità tra il farmaco vendibile senza obbligo di prescrizione medica (SOP) e altri farmaci precedentemente assunti)"*.

Per strutturare eventuali soluzioni informatiche in base a questa logica modulare il FSE appare necessaria una collaborazione tra informatici ed esperti in ambito sanitario.

La modularità deve essere coniugata anche con una dimensione di durata temporale, in base al principio che l'accesso ai dati personali del paziente deve essere giustificato da una necessità oggettiva di trattamento[34].

Integrazioni non modificative dell'originale

È interessante rilevare, anche ai fini dello sviluppo di applicativi per la gestione del FSE, che deve essere prevista, nel caso in cui l'interessato faccia uso del proprio diritto di procedere a integrazione, aggiornamento e rettificazione dei dati, deve essere **conservato l'originale** dei dati modificati e la

---

[33] Cfr. *Linee guida FSE cit.*.

[34] Garante, *Linee guida FSE*: *"In ogni caso, l'accesso al FSE/dossier deve essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali è abilitato il soggetto che accede. Ciò, comporta che i soggetti abilitati all'accesso devono poter consultare esclusivamente i fascicoli/dossier riferiti ai soggetti che assistono e per il periodo di tempo in cui si articola il percorso di cura per il quale l'interessato si è rivolto ad essi"*.

modifica apparire come documento aggiunto al primo[35].

<u>Elementi di cui tenere conto nella gestione informatica del FSE</u>

Nella progettazione del sistema software devono essere studiate procedure per consentire agli interessati di controllare i diritti di accesso ai dati sanitari, autorizzando oppure no alcuni soggetti o alcune categorie di soggetti, come anche di oscurare alcune informazioni e di variare tali scelte.

Allo stesso modo deve essere previsto un meccanismo efficace per **tenere traccia** dell'origine dei dati sanitari. Sul punto, il Garante nelle sue Linee guida sul FSE ha espressamente osservato: *"...Provenendo i dati sanitari e i documenti riuniti nel FSE da più soggetti, devono essere adottate idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del FSE"*.

Vanno anche implementati (come parte dell'argomento precedente) meccanismi di tracciamento dei **log** relativi non solo agli accessi al FSE, ma anche alle operazioni compiute[36].

Tra i diritti dell'interessato c'è anche quello di **estrarre copia del FSE**. Anche in tal senso, l'applicativo deve permettere di svolgere tale operazione con semplicità ed efficienza.

L'alimentazione del FSE e informazioni contenute

L'alimentazione del FSE avviene in maniera continuativa. I dati provengono da:

- i <u>soggetti che prendono in cura l'assistito</u> nell'ambito del Servizio sanitario nazionale e dei servizi socio-sanitari regionali[37];
- dallo <u>stesso paziente</u>, con i dati medici in suo possesso (su richiesta dello stesso paziente).

Il nucleo minimo del FSE è costituito dai seguenti documenti sanitari:

- referti;
- verbali Pronto Soccorso;
- lettere di dimissione;

---

[35] Garante, *cit.*: *"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 può essere fornito annotando le modifiche richieste senza alterare necessariamente la documentazione di riferimento"*.

[36] WP29_EHR, p. 20: *"(..T)he legal framework concerningsecurity measures should especially foresee the necessity of comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization"*.

[37] Si tratta ad es. di referti di laboratorio, radiologia e specialistica ambulatoriale.

- profilo Sanitario Sintetico[38];

Tale nucleo minimo può essere ampliato da ulteriore documentazione, quale:

- prescrizioni (specialistiche, farmaceutiche, ecc.);
- cartelle cliniche di ricovero (ordinario e day hospital);
- bilanci di salute;
- assistenza domiciliare: scheda, programma e cartella clinica;
- piani terapeutici;
- assistenza residenziale e semiresidenziale: scheda multidimensionale di valutazione;
- erogazione farmaci;
- certificati[39].

Il FSE deve consentire all'assistito, attraverso idonee funzionalità, di:

- esprimere le proprie determinazioni in materia di donazione di organi, previa informativa specifica, e possibilità di registrare in ogni momento variazioni di tale volontà, con relativa registrazione temporale[40].

Va rilevato che *"i dati anagrafici non fanno parte del FSE ma sono gestiti in* ***archivi separati*** *alimentati dalle anagrafi degli assistiti"* (cfr. Linee guida ministeriali 2010, p. 10). Si sottolinea il passaggio, che deve essere osservato nella progettazione di software per la gestione del FSE.

Taccuino personale del cittadino

Interessante infine notare che le Linee guida ministeriali del 2010 suggeriscono di prevedere nell'ambito del FSE il cosiddetto *"****taccuino personale del cittadino****"*, ossia *"una sezione riservata*

---

[38] *"La scheda sanitaria individuale è il contenuto informativo dell'applicativo di cartella clinica del MMG/PLS [medico di medicina generale / pediatra di libera scelta] da cui estrarre i dati che compongono il Patient Summary o 'Profilo Sanitario Sintetico'. Si definisce Patient Summary o Profilo Sanitario Sintetico il documento informatico sanitario che riassume la storia clinica del paziente e la sua situazione corrente. Tale documento è creato ed aggiornato dal MMG/PLS ogni qualvolta intervengono cambiamenti da lui ritenuti rilevanti ai fini della storia clinica del paziente e, in particolare, contiene anche un set predefinito di dati clinici significativi utili in caso di emergenza. Lo scopo del documento Profilo Sanitario Sintetico è quello di favorire la continuità di cura, permettendo un rapido inquadramento del paziente al momento di un contatto non predeterminato come ad esempio in situazioni di emergenza e di pronto soccorso"*, cfr. Linee guida ministeriali FSE 2010, p. 13.

[39] Si confronti per tale elencazione del nucleo minimo del FSE e degli altri documenti aggiuntivi le citate linee guida ministeriali 2010, pp. 12-13.

[40] Ved. Linee guida ministeriali cit., p. 16. Ai sensi della normativa vigente, l'assistito esprime la propria volontà in materia di donazione di organi attravero il medico di famiglia (art. 23, co. 3, l. n. 91/1999) o con nota scritta che contenga nome, cognome, data di nascita, dichiarazione di volontà (positiva o negativa), data e sottoscrizione (art. 1, co. 2 d.m. 8 aprile 2000).

al cittadino per offrirgli la possibilità di inserire dati ed informazioni personali (es. dati relativi al nucleo familiare, dati sull'attività sportiva, ecc.), file di documenti sanitari (es. referti di esami effettuati in strutture non convenzionate, referti archiviati in casa), un diario degli eventi rilevanti (visite, esami diagnostici, misure dei parametri di monitoraggio), promemoria per i controlli medici periodici. Questo consente di arricchire il FSE con ulteriori informazioni al fine di completare la descrizione dello stato di salute, ma tali informazioni e/o documenti risulteranno 'non certificate'”[41].

Un software dedicato al funzionamento del FSE dovrebbe perciò tenere in considerazione tali elementi ed essere strutturato in modo adeguato alla loro gestione, prevedendo anche uno spazio eventuale dedicato al “taccuino personale del cittadino” e gestendo i livelli di accesso a ciascuna parte del FSE.

Specifiche tecniche: piena interoperabilità nella consultazione e altre caratteristiche

Il comma 6-bis dell'art. art. 12 del d.l. 179/12 stabiliva che i decreti del Ministero della Salute previsti al comma 7 della stessa disposizione indicassero anche le modalità da osservare per la consultazione da parte del cittadino dei dati personali contenuti nel FSE *“in forma protetta e riservata”* e le modalità intese a garantire la **piena interoperabilità** tra *“interfacce, sistemi e applicazioni software”* adottate.

A tal proposito, il comma 7, art. 12 d.l. 179/12 in commento chiariva che i regolamenti, inoltre, avrebbero determinato i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività.

I decreti dovevano inoltre intervenire sui seguenti punti:

- contenuti del FSE;
- limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione;
- sistemi di codifica dei dati;
- garanzie e misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito;
- modalità e livelli diversificati di accesso al FSE da parte del Servizio Sanitario Nazionale e

---

[41] Linee guida ministeriali FSE, p. 16.

dei Servizi Soci-sanitari regionali (per le finalità di cura) e delle Regioni, delle Province autonome, del Ministero del lavoro e delle politiche sociali, del Ministero della salute (per le finalità di ricerca scientifica e amministrative);

- definizione delle modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato.

Il D.L. 21 giugno 2013, n. 69, convertito con modificazioni dalla L. 9 agosto 2013, n. 98, ha disposto poi:

- (con l'art. 13, comma 2-bis) che "*I regolamenti previsti dagli articoli 2, comma 5, 3, comma 4, 12, comma 13, e 14, comma 2-bis, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, qualora non ancora adottati e decorsi ulteriori trenta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono adottati su proposta del Presidente del Consiglio dei ministri*";
- (con l'art. 13, comma 2-quater) che i decreti ministeriali previsti dal comma 7 dell'art. 12 D.L. 179/2012, qualora non ancora adottati e decorsi ulteriori trenta giorni dalla data di entrata in vigore della legge di conversione del D.L. medesimo, fossero adottati dal Presidente del Consiglio dei ministri anche ove non sia pervenuto il concerto dei Ministri interessati.

E, in effetti, proprio con il DPCM 29 settembre 2015, n. 178, ha visto la luce il Regolamento tecnico in materia di FSE (si veda *supra*, art. 23 per le misure di sicurezza in materia di protezione dei dati personali).

In materia di principi tecnici ai quali attenersi nella costruzione del FSE, è opportuno evidenziare che le già citate Linee guida ministeriali del 2010 sollecitavano l'adesione a **standard internazionali di progettazione**, con adozione di *"sistemi di codifica che presentano le seguenti caratteristiche:*

- *l'esaustività: ogni oggetto deve trovare posto in una delle classi;*
- *l'economicità: un numero relativamente ridotto di codici consente di rappresentare un numero più grande di contenuti informativi;*
- *l'orientamento ad un fine: i criteri di costituzione delle classi sono arbitrari e dipendono,*

per ogni classificazione, dai fini della classificazione stessa;

- *la mutua esclusività: ogni oggetto deve essere classificabile in modo univoco in una sola classe"*[42].

Viene in tal senso evidenziato nelle citate Linee guida che *"si rende necessario definire modalità di rappresentazione delle informazioni che siano consistenti ed interpretabili dai sistemi coinvolti con l'utilizzo di informazioni codificate grazie all'uso di* ***nomenclatori definiti e condivisi a livello nazionale****"* (cfr. p. 17). Nella scelta e nella progettazione di sistemi di gestione del FSE è pertanto indispensabile partire da una ricognizione relativa all'interoperabilità con i sistemi già in uso e procedere a una corretta ricognizione preliminare dei nomenclatori da utilizzare. Le Linee guida del 2010 menzionavano in questo senso anche che gli standard vigenti come l'HL7 (cfr. parte generale di questo lavoro, in riferimento agli standard di codifica in materia di sanità elettronica).

Occorre altresì considerare, che nella scelta del software di gestione del FSE dovrebbero essere privilegiate quelle soluzioni che non si basano sulla costituzione di un nuovo database, quanto piuttosto realizzano collegamenti ***on the fly*** tra database già esistenti, in modo da presentare (in maniera aggiornata) tutti gli eventi sanitari che hanno interessato il paziente e la cui evidenziazione nel contesto unitario del FSE è stata consentita dal paziente. Il punto emerge dalle Linee guida emanate dal Garante privacy: *"Il FSE deve essere costituito preferendo, di regola, soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l'interessato"*. Questa preferenza per un tipo di architettura software che eviti la riproduzione di un database dovrebbe rappresentare perciò un elemento chiave da tenere presente in fase di sviluppo software.

ASPETTI RELATIVI ALLA SCELTA DEI FORNITORI DELLE INFRASTRUTTURE DI FSE / DSE

Con riferimento alla scelta delle infrastrutture, si dirà brevemente quanto segue:

- il trattamento di dati personali in ambito di sanità elettronica, in generale, non sembra porre particolari problemi in termini di scelta delle infrastrutture (e, quindi, del fornitore) se non quelli legati al rispetto dei requisiti tecnici previsti dalla normativa applicabile a seconda dei vari soggetti (es. enti sanitari pubblici, convenzionati o privati);

---

[42] Cfr. Linee guida ministeriali 2010 FSE, p. 17.

- con riferimento al solo FSE, tuttavia, risulta evidente che il legislatore abbia voluto prevedere come uniche possibilità per la sua realizzazione quelle di collocarlo o sull’infrastruttura propria delle Regioni o Province Autonome interessate o sull’infrastruttura nazionale di interoperabilità di cui all’art. 12 comma 15 del D.L. 179/2012. Ciò è corroborato anche dalla lettura dell’art. 27 del DPCM 178/2015 e della regola n. 6.1 del Disciplinare tecnico a quest’ultimo allegato. In buona sostanza, la conseguenza di tale interpretazione depone nel senso che un gruppo di strutture sanitarie non potrebbe realizzare il “proprio” FSE mediante appalto a fornitori scelti distintamente da quelli che, ufficialmente, forniscono già l’infrastruttura sanitaria alla Regione o Provincia Autonoma in cui operano o l’infrastruttura nazionale di interoperabilità. Tradotto in altre parole, l’unico FSE possibile, sul piano della legittimità di fondo, è solo ed esclusivamente quello previsto *ex lege* e insistente sulle infrastrutture sanitarie pubbliche (regionali, provinciali autonome o nazionale di interoperabilità);
- diverso è il caso dei dossier sanitari elettronici, interni quindi ad un solo titolare del trattamento (sia esso una ASL, un ospedale, una clinica, ecc.), che ben potranno essere realizzati su infrastruttura realizzata e mantenuta da fornitori scelti dal singolo soggetto titolare;
- ancora diverso, ma rilevantissimo alla luce della necessaria e piena attuazione del cd. Decreto Balduzzi (D.L. 13 settembre 2012, n. 158, convertito in legge, con modificazioni, dall’art.1, comma 1, L. 8 novembre 2012, n. 189), l’ambito delle cosiddette “aggregazioni funzionali territoriali” e delle “unità complesse di cure primarie”, che implica a vari livelli la condivisione di informazioni sanitarie strutturate, relative ad assistiti, tra più soggetti operanti su uno stesso territorio. Sul punto, dopo un primo periodo di difficile orientamento, è intervenuto con il paragrafo 4 delle Linee guida sul Dossier sanitario [cfr. pag. 17, GarDS] il Garante privacy, chiarendo che tali banche dati condivise non possono essere considerate né alla stregua di meri DSE, né qualificati come FSE. Anche alla luce di tale lettura, si deve concludere che, in tali casi, ben potranno i soggetti coinvolti a vario titolo nell’offerta di servizi territoriali di assistenza primaria selezionare fornitori tecnologici, anche in modalità “cloud”, che realizzino e mantengano le infrastrutture connesse a questi specifici servizi integrati, sempre che si rispettino le numerose norme in materia di protezione dei dati personali e le misure prescritte dal Garante stesso, con le menzionate GarFSE e GarDS.

PARTE QUARTA

Vademecum sintetico per singoli documenti sanitari d'uso comune, non condivisi in dossier o fascicolo sanitario elettronico, che possono essere realizzati con software di lavoro “classici” per l'ufficio basati su tecnologia di cloud computing

Possiamo sintetizzare di seguito le cautele in materia di protezione dei dati personali (D.lgs. 196/2003) e cloud computing, con riferimento alla realizzazione di singoli documenti di uso comune in ambito sanitario e clinico. Per ciascuna categoria, si evidenziano sommariamente i principali “punti di attenzione privacy” da tenere presenti, in caso di utilizzo di software “classici” d'ufficio basati su piattaforme cloud di tipo pubblico e/o privato e/o ibrido.

PRENOTAZIONI

Liste di attesa
Diagnostica
Specialistica ambulatoriale

Trattandosi di gestione amministrativa continuativa e in rete di dati personali anche idonei a rivelare lo stato di salute o comunque sensibili dei pazienti (e/o dei loro famigliari), per finalità connesse alla prenotazione delle prestazioni di prevenzione/diagnosi/cura/riabilitazione, l'adozione di una tecnologia applicativa d'ufficio basata su piattaforma di cloud computing pubblico internazionale (software as as service) non appare la più idonea. In ogni modo, è bene privilegiare soluzioni di private cloud o, in alternativa, un'offerta di public cloud che garantisca la permanenza dei dati all'interno dell'Unione Europea (data center collocati in uno o più degli Stati Membri) oppure, ancora, richiedere il consenso al trasferimento internazionale dei dati a ciascun interessato, per la particolare natura delle documentazioni di tale pratiche che – spesso – confluiscono come fonti in sistemi di fascicolazione sanitaria elettronica (FSE). Va rammentato, in riferimento a quest'ultima modalità di organizzazione dell'intera storia sanitaria del paziente, che il gruppo dei Garanti europei sconsiglia comunque il trasferimento dei dati in paesi esterni all'Unione europea o inadeguati dal punto di vista delle garanzie offerte in materia di protezione dei dati personali; tale scelta di mantenimento dei dati personali intra-UE o in paesi ritenuti adeguati sotto il profilo privacy dovrebbe quindi essere preferita, in via prudenziale, anche all'acquisizione di un consenso specifico dell'interessato al trasferimento. Resta ferma la necessità di adottare sistemi che rendano possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato (es. https). Si sottolinea in particolare la necessità di rispettare la misura della separazione tra elemento identificativo del dato personale e informazione sanitaria, anche avvalendosi – nel caso – di opportune soluzioni software per agevolare e automatizzare il processo di separazione (eventualmente integrabili nel servizio acquistato). Nell'utilizzo di soluzioni di tipo ufficio, particolare cura infine deve essere posta ad elementi potenzialmente idonei a determinare variazioni nel testo dei documenti informatici prodotti, come funzioni “macro” o particolari codici di campo. Occorre inoltre considerare con attenzione la possibile vulnerabilità informatica degli strumenti informatici utilizzati. Quanto alle caratteristiche di funzionamento e robustezza del cloud da utilizzare, si suggerisce, infine, di effettuare le necessarie verifiche su parametri essenziali di funzionamento, quali le garanzie di continuità operativa, disaster recovery, interoperabilità anche rispetto a sistemi già attivi, portabilità dei dati, prestando particolare attenzione ai Service level agreement (SLA). Deve infatti ritenersi che tali requisiti, per ciò che interessa il presente vademecum, rientrino anche nel novero delle misure di sicurezza. Può risultare opportuno, come indicato dal Garante per la protezione dei dati personali, mantenere una copia “locale” dei dati sanitari, qualora le garanzie in materia di disaster recovery non appaiano del tutto soddisfacenti.

REGISTRI

Pazienti cronici

Assistenza integrativa

ADI / ADP

Malattie rare

L'utilizzo di software d'ufficio basati su piattaforma di cloud computing pubblico per la creazione/elaborazione di registri di pazienti/assistiti – ferme restando le cautele previste per determinate informazioni relative a malattie specifiche – appare legittimo se il sistema informatico rende possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato (es. https). Va sottolineata l'importanza di procedere alla conservazione separata dell'elemento identificativo rispetto a quello dell'informazione sanitaria. In caso di utilizzo di sistemi che sfruttino risorse tecnologiche collocate fuori dall'Unione Europea, sarebbe opportuno richiedere il consenso all'interessato o affidarsi unicamente a fornitori che accettino di stipulare le Clausole Standard (Model Clause) per il corretto trasferimento dei dati all'estero, approvate dalla Commissione Europea il 5 febbraio 2010, oppure a fornitori collocati solo in Paesi considerati sicuri dall'Unione Europea (es. Canada, Svizzera, ecc.) che accettino la designazione a Responsabile del trattamento e i connessi obblighi. Per la naturale conformazione delle filiere di sub-fornitori tipiche dei servizi di cloud computing internazionale, non sembrano strumenti giuridici sufficienti, per il momento, le Norme vincolanti d'impresa (Binding corporate rules) né il programma *Privacy Shield*. Invece, con riferimento all'eventuale successivo uso dei registri nel contesto di una fascicolazione sanitaria elettronica, è necessario richiedere il consenso dell'interessato per l'utilizzo di sistemi cloud-based collocati fuori dall'Unione Europea. Si ripete, ad ogni buon conto, la raccomandazione già espressa nella scheda precedente ad evitare, di preferenza, soluzioni cloud in materia di fascicolo sanitario elettronico e di dossier sanitario elettronico che comportino un trasferimento dei dati in paesi extra UE che non offrano un livello adeguato di protezione dei dati personali. Come evidenziato nella scheda precedente, attenzione particolare andrebbe prestata a fattori quali le garanzie in materia di continuità operativa, disaster recovery, interoperabilità dei sistemi e portabilità dei dati, potendo tali elementi essere considerati anche misure di sicurezza in ambito privacy, dal momento che garantiscono tra l'altro l'integrità dei dati, la loro modificabilità, la loro corretta lettura, il controllo dell'interessato. Alcuni dei registri indicati possono altresì riportare dati genetici, il che rende necessaria l'adozione di particolari misure di autenticazione forte (*strong authentication*), di cui è necessario valutare la disponibilità al momento della scelta del cloud o la possibilità di integrazione con il servizio cloud scelto.

RIEPILOGHI/REPORT

Nominativi

Anonimi

L'adozione di software as a service basati su cloud computing pubblico per la realizzazione/elaborazione di riepiloghi/report anonimi è perfettamente legittima e non richiede particolari accortezze in materia di protezione dei dati personali. È necessario che le soluzioni tecniche previste assicurino un reale anonimato, ossia l'impossibilità di riconversione in dato personale.

Come per i registri, anche in caso di riepiloghi/report nominativi è necessario che il sistema informatico renda possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato (es. https). Come per i registri, anche per i riepiloghi/report nominativi, in caso di utilizzo di sistemi che sfruttino risorse tecnologiche collocate fuori dall'Unione Europea, sarebbe opportuno richiedere il consenso all'interessato o affidarsi unicamente a fornitori che accettino di stipulare le Clausole Standard (Model Clause) approvate dalla Commissione Europea il 5 febbraio 2010, oppure rivolgersi a fornitori collocati solo in Paesi considerati sicuri dall'Unione Europea (es. Canada, Svizzera, ecc.) che accettino la designazione a Responsabile del trattamento e i connessi obblighi. Per la naturale conformazione delle filiere di sub-fornitori tipiche dei servizi di cloud computing internazionale, non sembrano strumenti giuridici sufficienti, per il momento, le Norme vincolanti d'impresa (Binding corporate rules) né il programma *Privacy Shield*. Invece, con riferimento all'eventuale successivo uso dei riepiloghi/report nel contesto di una fascicolazione sanitaria elettronica, è necessario richiedere il consenso dell'interessato per l'utilizzo di sistemi di storage cloud-based collocati fuori dall'Unione Europea, sebbene si ripeta anche in questa scheda come nelle precedenti che il trasferimento extra UE o verso paesi inadeguati sotto il profilo privacy è da ritenersi in ogni caso sconsigliato. Si richiama quanto evidenziato nella scheda precedente a proposito di interoperabilità, portabilità, continuità operativa e disaster recovery.

IMMAGINI

Nominative

Anonime

L'adozione di software as a service basati su cloud computing pubblico per la realizzazione/elaborazione di immagini anonime è perfettamente legittima e non richiede particolari accortezze in materia di protezione dei dati personali, purché si tratti di anonimato irreversibile. Come per i registri, in caso di immagini nominative, è necessario che il sistema informatico renda possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato (es. https). Come per i registri, anche per le immagini nominative, in caso di utilizzo di sistemi che sfruttino risorse tecnologiche collocate fuori dall'Unione Europea, sarebbe opportuno richiedere il consenso all'interessato o affidarsi unicamente a fornitori che accettino di stipulare le Clausole Standard (Model Clause) approvate dalla Commissione Europea il 5 febbraio 2010, oppure rivolgersi a fornitori collocati solo in Paesi considerati sicuri dall'Unione Europea (es. Canada, Svizzera, ecc.) che accettino la designazione a Responsabile del trattamento e i connessi obblighi. Per la naturale conformazione delle filiere di sub-fornitori tipiche dei servizi di cloud computing internazionale, non sembrano strumenti giuridici sufficienti, per il momento, le Norme vincolanti d'impresa (Binding corporate rules) né il programma *Privacy Shield*. Invece, con riferimento all'eventuale successivo uso delle immagini nel contesto di una fascicolazione sanitaria elettronica, è necessario richiedere il consenso dell'interessato per l'utilizzo di sistemi di storage delle immagini cloud-based collocati fuori dall'Unione Europea, sebbene comunque tale scelta di trasferimento extra UE o verso paesi non sicuri sotto il profilo privacy sia da sconsigliare. Valgono le indicazioni già espresse nelle schede precedenti a proposito dei requisiti dell'interoperabilità, portabilità, continuità operativa, disaster recovery, che hanno rilevanza anche in ambito privacy oltreché strettamente amministrativo.

DOCUMENTI CLINICI

SDO
Lettera dimissione
Certificati
Referti
Ricette
Patient Summary
Cartella clinica

L'adozione di software as a service basati su cloud computing pubblico per la realizzazione/elaborazione di singoli documenti clinici appare in astratto legittima ma impone che il sistema informatico renda possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato (es. https). Come per i registri, anche per i documenti clinici, in caso di utilizzo di sistemi che sfruttino risorse tecnologiche collocate fuori dall'Unione Europea, sarebbe opportuno richiedere il consenso all'interessato o affidarsi unicamente a fornitori che accettino di stipulare le Clausole Standard (Model Clause) approvate dalla Commissione Europea il 5 febbraio 2010, oppure rivolgersi a fornitori collocati solo in Paesi considerati sicuri dall'Unione Europea (es. Canada, Svizzera, ecc.) che accettino la designazione a Responsabile del trattamento e i connessi obblighi. Nel caso di cartelle cliniche elettroniche / dossier sanitari elettronici, fascicolo sanitario elettronico, quest'ultima soluzione, ossia il mantenimento dei dati sanitari in paesi che garantiscono un adeguato livello di protezione dei dati personali, è da considerarsi assolutamente preferibile rispetto a scelte che, pur in presenza del consenso dell'interessato al trasferimento estero, comportino comunque uno storage in paesi considerati non adeguati sotto il profilo della normativa privacy. Per la naturale conformazione delle filiere di sub-fornitori tipiche dei servizi di cloud computing internazionale, non sembrano strumenti giuridici sufficienti, per il momento, le Norme vincolanti d'impresa (Binding corporate rules) né il programma *Privacy Shield*. Invece, con riferimento all'eventuale successivo uso dei documenti clinici nel contesto di una fascicolazione sanitaria elettronica, è necessario richiedere il consenso dell'interessato per l'utilizzo di sistemi di storage cloud-based collocati fuori dall'Unione Europea. Occorre prestare particolare attenzione alle norme specifiche vigenti in relazione a ciascuno degli strumenti indicati, per le quali si rimanda anche alla parte generale di questo scritto. Come già osservato nelle schede precedenti, particolare attenzione deve essere prestata alle garanzie offerte dal fornitore di cloud in materia di continuità operativa, disaster recovery, interoperabilità tra sistemi, portabilità dei dati, effettuando verifiche opportune anche rispetto alle SLA eventualmente fornite con il contratto. Deve infatti ritenersi che tali requisiti abbiano incidenza anche in materia di tutela dei dati personali.

COMUNICAZIONI VERSO L'UTENZA E/O I PAZIENTI INTERESSATI

Personali - Impersonali

L'utilizzo di siti web “vetrina” che non comportano diffusione e/o comunicazione di dati personali sensibili (per esempio siti utilizzati per informazioni amministrative, es. indirizzi e orari di apertura di sportelli di aziende sanitarie o farmacie) non implica significative problematiche in ordine all'adozione di sistemi basati su piattaforme di cloud computing internazionale pubblico.

In caso, viceversa, di siti che consentano il download on line oppure di utilizzo di client di posta elettronica cloud-based per l'invio di referti o altra documentazione contenente dati personali idonei a rivelare lo stato di salute, si raccomanda di adottare sistemi che rendano possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati – oltre all'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 – anche la gestione delle restanti misure tecnologiche di sicurezza previste in materia di refertazione on line dal Garante italiano per la protezione dei dati personali con le Linee Guida del 19 novembre 2009, già specificate nel presente manuale e qui di seguito richiamate:

Per consultazione tramite web

1. utilizzo di protocolli con standard crittografici e certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https tls/ssl);
2. evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;
3. autenticazione sicura dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
4. disponibilità limitata nel tempo del referto on-line (massimo 45 gg.);
5. controllo dell'interessato: facoltà di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.
6. Procedure di sicurezza che rendono immediatamente non disponibili per la consultazione on-line i referti relativi a un interessato che abbia comunicato la compromissione della sicurezza delle proprie credenziali di autenticazione

Spedizione del referto tramite posta elettronica

1. Spedizione del referto in forma di allegato a un messaggio e-mail e non come testo compreso nella body part del messaggio;
2. password o chiave crittografica per l'apertura del file rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B al Codice). Questa cautela può essere disapplicata su richiesta

dell'interessato.
3. convalida degli indirizzi e-mail tramite apposita procedura di verifica online, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.
4. procedure di sicurezza che interrompono immediatamente l'invio per posta elettronica dei referti relativi a un interessato che abbia comunicato la compromissione della sicurezza delle proprie credenziali di autenticazione

In caso di utilizzo di sistemi che sfruttino risorse tecnologiche collocate fuori dall'Unione Europea, sarebbe opportuno richiedere il consenso all'interessato o affidarsi unicamente a fornitori che accettino di stipulare le Clausole Standard (Model Clause) approvate dalla Commissione Europea il 5 febbraio 2010, oppure rivolgersi a fornitori collocati solo in Paesi considerati sicuri dall'Unione Europea (es. Canada, Svizzera, ecc.) che accettino la designazione a Responsabile del trattamento e i connessi obblighi. Particolare attenzione va posta anche in questo caso alle garanzie offerte dal fornitore di cloud in materia di continuità operativa, disaster recovery, interoperabilità tra sistemi, portabilità dei dati, effettuando verifiche opportune anche rispetto alle SLA eventualmente fornite con il contratto.

PRATICHE
Esenzioni
Presidi / protesica
Assistenza indiretta
Scelta / revoca MMG – PLS

Trattandosi di gestione amministrativa continuativa e in rete di dati personali anche idonei a rivelare lo stato di salute o comunque sensibili dei pazienti (e/o dei loro famigliari), per finalità di richiesta di assistenza e/o presidi strettamente connessi prestazioni di prevenzione/diagnosi /cura /riabilitazione, l'adozione di una tecnologia applicativa d'ufficio basata su piattaforma di cloud computing pubblico internazionale (software as as service) non appare la più idonea, fatto salvo per quanto concerna i sistemi di scelta via web del MMG – PLS che non sembrano presentare particolari criticità (ferma restando, anche in tale ultimo caso, la necessità di adottare sistemi che rendano possibile al Cliente-Titolare del trattamento e agli utenti da esso incaricati l'impostazione di tutte le misure di sicurezza previste dall'Allegato B al D.Lgs. 196/2003 e del protocollo di trasmissione delle informazioni cifrato, es. https). In ogni modo, è bene privilegiare soluzioni di private cloud o, in alternativa, un'offerta di public cloud che garantisca la permanenza dei dati all'interno dell'Unione Europea (data center collocati in uno o più degli Stati Membri) oppure, ancora, richiedere il consenso al trasferimento internazionale dei dati a ciascun interessato, per la particolare natura delle documentazioni di tale pratiche che – spesso – confluiscono come fonti in sistemi di fascicolazione sanitaria elettronica. Si raccomanda, come in precedenza, di valutare attentamente le garanzie offerte dal fornitore di cloud in materia di continuità operativa, disaster recovery, interoperabilità tra sistemi, portabilità dei dati, effettuando verifiche opportune anche rispetto alle SLA eventualmente fornite con il contratto.

PARTE QUINTA – CHECKLIST PRIVACY

La seguente Checklist è aggiunta come strumento pratico per riassumere e verificare i più significativi requisiti discussi in questo manuale. E' stata concepita per essere utilizzata dai fornitori cloud che desiderano offrire i propri servizi ad operatori sanitari pubblici italiani, ma può anche risultare utile a questi ultimi come lista di riferimenti pratici, a cui ricorrere nella fase di trattativa contrattuale con fornitori di servizi di cloud computing.

	SaaS	PaaS	IaaS
1. Sono applicate/applicabili le misure di sicurezza indicate negli articoli 22, 31-34 del Codice privacy italiano (D.Lgs. 196/2003), nel suo Allegato B, nel Provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema? S= OK / N= non-compliance	X	X**	X***
1.1. In particolare, sono applicate/applicabili le specifiche misure riguardanti il mantenimento della Continuità Operativa? S= OK / N= non-compliance	X	X	X
1.2. In particolare, sono applicate/applicabili le specifiche misure riguardanti effettive soluzioni di disaster recovery? S= OK / No= non-compliance	X	X	X
1.3. In particolare, sono applicate/applicabili specifiche misure finalizzate a prevenire accessi abusivi ai sistemi? S= OK / N= non-compliance	X	X	X
1.4. In particolare, i dati sono cancellati completamente a richiesta del Cliente o al termine del servizio (eccetto per ciò che concerne il servizio di portabilità)? S= OK / N= non-compliance	X	X	X
2. Sono applicate/applicabili misure che assicurano l'esercizio dei diritti degli interessati elencati all'art. 7 del Codice privacy italiano? S= OK / N= non-compliance	X*	X**	X***
2.1. Le istanze di accesso ai dati degli interessati trovano risposta entro 15 giorni (o al massimo entro 30 giorni in casi più complessi) dalla richiesta? S= OK / N= non-compliance	X*	X**	X***
3. La portabilità dei dati è garantita, sia dal punto di vista contrattuale sia sul versante tecnologico? S= OK / N= non compliant	X	X	X
4. L'interoperabilità dei sistemi è pienamente garantita dal fornitore? S= OK / N= non compliant	X	X	X
5. Il servizio rende possibile una involontaria modifica automatica di dati attraverso l'uso di macro/fields/ecc.? S= non-compliance / N= OK	X	X**	–
6. Sono specificati i costi totali dei servizi (inclusi installazione, manutenzione, supporto)? S= pro / N= contro	X	X	X
7. Può il fornitore cloud rilasciare prove ed evidenze della propria affidabilità organizzativa ed economica, mediante report, bilanci, ecc.? S= pro / N= contro	X	X	X
8. Il cloud provider possiede certificazioni riconosciute internazionalmente (es. ISO)? S= pro / N= contro	X	X	X
9. Il cloud provider non tratta i dati caricati dal Cliente per finalità proprie? S= OK / N= non-compliance	X	X	X
10. Le giurisdizioni e leggi applicabili sono chiaramente indicate nei contratti? S=pro / N =contro	X	X	X
10.1. Le giurisdizioni e leggi applicabili sono conformi alla normativa vigente (è stato eseguito un controllo di legittimità)? S= OK / N= non-compliance	X	X	X
11. Al contratto è allegato un Service Level Agreement in linea con gli standard di mercato? S= pro /	X	X	X

N= contro			
12. Il servizio mantiene i dati all'interno dell'Unione Europea? S= OK / N= leggere specifiche di seguito	X	X	X
12.1. Il Paese extra-UE di destinazione è considerato adeguato o il fornitore, se USA, è certificato “*Privacy Shield*”? S = OK / N = leggere sotto	X	X	X
12.1.2. Il fornitore extra-UE adotta le Clausole standard approvate dalla Commissione Europea per il corretto trasferimento dei dati personali all'estero? S = OK / N = leggere sotto	X	X	X
12.1.2.3. Se non ricorre nemmeno una delle condizioni di cui sopra, gli interessati a cui si riferiscono i dati hanno dato specifico consenso al trasferimento all'estero degli stessi (o vi sono altre esenzioni/cause di legittimazione)? S= OK / N= non-compliance	X*	X**	—
13. Il servizio cloud è adottato per trattare dati sulla salute? S= leggere sotto / N=OK	X	X	X
13.1. Il servizio offre strumenti al Cliente perché questo possa separare i dati sulla salute dai restanti dati personali? S= OK / N= non-compliance	X*	X**	—
13.2. Il servizio consente in qualche modo di impedire un accesso diretto/immediato da parte del personale che opera sul sistema (per esempio con cifrature)? S= OK / N= non-compliance	X*	X**	X
13.3. Il servizio consente il trasferimento telematico di dati sulla salute attraverso connessioni cifrate? S=OK / N= non-compliance	X	X	X
13.4. I dati sulla salute possono essere diffusi e resi accessibili a soggetti terzi indeterminati? S= non-compliance / N= OK	X	X	X
14. Il servizio cloud è adottato per trattare dati genetici? S= leggere sotto / N=OK	X	X	X
14.1. Sono applicate/applicabili misure che consentono l'accesso ai dati genetici solo attraverso “autenticazione forte” anche biometrica? S= OK / N= non-compliance	X	X	X
14.2. Sono applicate/applicabili procedure per separare, al momento della raccolta dei dati genetici, le informazioni identificanti dalle informazioni genetiche? S= OK / N= non-compliance	X*	X**	—
14.3. E' possibile applicare una firma digitale conforme ai sensi della legge italiana prima dell'invio di dati genetici attraverso posta elettronica certificata? S= OK / N= non-compliance	X*	X**	—
14.4. Nel caso dei dati genetici che sono anche dati sulla salute, tutte le condizioni elencate al precedente punto 13 sono soddisfatte? S= OK / N= non-compliance	X	X	X
15. Il servizio consente il trattamento di formati sanitari internazionali (HL7, EN 13606, openEHR...)? S= OK / N= contro	X*	X**	—
16. Il servizio verrebbe usato per gestire referti on line? S= leggere sotto / N= OK	X*	X**	—
16.1. Sono rispettabili tutte le norme rilevanti (si legga il Manuale nella parte dedicata ai Referti On line)? S= OK / N= non-compliance	X*	X**	—
17. Il servizio verrebbe usato per gestire il Fascicolo Sanitario Elettronico (FSE) o un Dossier Sanitario Elettronico (DSE)? S= leggere sotto / N = OK	X	X	—
17.1. Il servizio mantiene il FSE/DSE all'interno dell'Unione Europea S= OK / N= leggere 17.2	X	X	—
17.2. E' richiesto un consenso agli interessati per il trasferimento dei dati di FSE/DSE fuori dall'Unione Europea? S= OK / N= non-compliance	X	X**	—
17.3. Il servizio rende possibile l'oscuramento selettivo dei dati contenuti nell'FSE/DSE? S= OK / N= non-compliance	X	X**	—
17.4. Il servizio rende possibile l'oscuramento del fatto stesso che sia stato applicato un oscuramento di determinati dati? S= OK / N= non-compliance	X	X**	—
17.5. Il servizio rende possibile la gestione di diversi profili di autorizzazione, in modo da rendere selettivamente accessibili I dati da parte dei diversi operatori coinvolti nei processi di cura, diagnosi, riabilitazione, prevenzione e amministrativi strettamente correlati ai precedenti?S= OK / N= non-compliance	X	X**	—
17.6. Il servizio rende possibile la registrazione dei log di chi abbia aggiunto/consultato dati e di quali dati siano stati aggiunti/consultati? S= OK / N= non-compliance	X	X**	—

S = Sì - N = No X = applicabile – = non applicabile

* = il Cliente potrebbe normalmente soddisfare questi requisiti da solo (per esempio usando altre applicazioni, le proprie procedure interne, ecc.)

** = Il servizio cloud potrebbe fornire le funzionalità per farlo, ma sta al Cliente applicare correttamente le misure

CONCLUSIONI

Le pagine che precedono illustrano in maniera sintetica e dettagliata un complesso di elementi di cui tenere conto nello sviluppo di servizi cloud per la sanità elettronica, si tratti di servizi di mero *storage* di dati sanitari o di più complessi applicativi per la gestione di specifici strumenti della sanità elettronica. Le indicazioni fornite sono di interesse non solo per gli sviluppatori (siano essi Pubbliche amministrazioni o fornitori privati) ma per le stesse Pubbliche amministrazioni committenti o utilizzatrici, dovendo esse verificare l'esistenza dei requisiti indicati nella fornitura dei servizi di cloud in ambito sanitario. Sarebbe ripetitivo riepilogare in questa parte conclusiva, sia pure sinteticamente, elementi già indicati in forma per lo più di “bullet” nelle pagine precedenti. Ugualmente, potrebbe creare asimmetrie richiamare solo alcuni di essi ai quali prestare speciale attenzione. Ci si limita pertanto a riepilogare la struttura logico-giuridica seguita in questo lavoro, solo perché potrebbe in effetti costituire una base metodologica di analisi di soluzioni cloud proposte. Si suggerisce perciò di:

1. esaminare innanzitutto in senso generale se ricorrono i requisiti previsti in generale nel Codice dell'amministrazione digitale, quelli indicati dal Garante per la protezione dei dati personali nella scelta di soluzioni cloud, quelli specifici che trovano applicazione all'ambito sanitario (cfr. prima parte di questo lavoro)
2. dal momento che le soluzioni cloud implicano, nella maggior parte dei casi (ma pur sempre con notevoli eccezioni, che dipendono anche dall'architettura utilizzata), un'ampia circolazione geografica dei dati sanitari, esaminare in maniera specifica se possono considerarsi soddisfatte le norme che disciplinano la circolazione dei dati sanitari e genetici (cfr. parte seconda di questo lavoro)
3. esaminare le caratteristiche di dettaglio relative al particolare strumento della sanità elettronica che si intende gestire attraverso il cloud, per verificarne la compatibilità normativa.

In linea generale, e conclusivamente, deve rilevarsi, dall'analisi normativa condotta, che pur con determinate cautele ed effettuando le opportune verifiche contrattuali, le soluzioni cloud **appaiono pienamente compatibili** con l'affidamento di moltoi servizi della sanità elettronica. Si raccomanda comunque di porre particolare attenzione alla **localizzazione** intra UE / SEE (o paese che offra adeguato livello di protezione) dei dati del FSE (specialmente nel servizio di *storage*). La cautela vale anche per i dossier sanitari e, deve ritenersi, per le cartelle cliniche elettroniche.