Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Analisi valutativa dell'adozione del Cloud per il Fascicolo Sanitario Elettronico

Angelo Esposito

RT-ICAR-NA-2013-01 **Marzo 2013**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) – Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: *www.na.icar.cnr.it*

Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Analisi valutativa dell'adozione del Cloud per il Fascicolo Sanitario Elettronico

Angelo Esposito[1]

Rapporto Tecnico N: **RT-ICAR-NA-2013-01** ***Data:*** **Marzo 2013**

---

[1] Istituto di Calcolo e Reti ad Alte Prestazioni, ICAR-CNR, Sede di Napoli, via P. Castellino, 111, 80131 Napoli.

Analisi valutativa dell'adozione del Cloud per il Fascicolo Sanitario Elettronico

Angelo Esposito

Istituto di Calcolo e Reti ad Alte Prestazioni, Consiglio Nazionale delle Ricerche
Via Pietro Castellino, 111 – 80131 Napoli, Italia
E-mail: angelo.esposito@na.icar.cnr.it

Abstract

L'uso del Cloud Computing per l'erogazione dei servizi del Fascicolo Sanitario Elettronico risulta di particolare interesse per gli enormi benefici portati dall'adozione di tale paradigma.

In questo lavoro, è stata svolta un'analisi valutativa dell'adozione del cloud nel contesto dei servizi del Fascicolo Sanitario Elettronico (FSE).

L'obiettivo dell'analisi è stato duplice, da una parte individuare le condizioni di successo all'uso del cloud, dall'altro prevedere l'applicazione del cloud nel contesto dell'e-health con possibili scenari architetturali.

Keywords: Cloud, Fascicolo Sanitario Elettronico, Interoperabilità.

1. Introduzione

Negli ultimi tre anni le iniziative volte alla realizzazione del Fascicolo Sanitario Elettronico (FSE) hanno coinvolto numerosi soggetti dell'amministrazione pubblica centrale, delle Regioni italiane, delle aziende sanitarie. Nell'ambito di tale contesto, sono molte le iniziative progettuali che hanno reso possibile l'interoperabilità delle soluzioni territoriali di FSE rendendo di fatto InFSE l'infrastruttura abilitante all'interoperabilità delle soluzioni di FSE territoriali.

Tra i progetti di maggiore rilevanza a livello nazionale ed europeo si citano quelli più importanti:

- Il progetto "Infrastruttura tecnologica del FSE": ha definito un modello architetturale dell'infrastruttura tecnologica, che definisce i meccanismi per la raccolta e disponibilità di documenti e dati sanitari in formato digitale e i servizi di supporto ai processi sanitari;
- Il progetto OpenInFSE: ha realizzato una prima rete tecnologica stabile a supporto dell'interoperabilità delle soluzioni territoriali di fascicolo sanitario elettronico. Tale rete è costituita da Aziende Ospedaliere, Aziende Sanitarie Locali e sistemi informativi territoriali di alcune Regioni e Province Autonome;
- Il progetto IPSE: ha come obiettivo lo scambio di documenti clinici, in particolare del Patient Summary e dell'ePrescription;
- Il progetto EPSOS: ha come obiettivo lo scambio di documenti clinici, in particolare del Patient Summary e dell'ePrescription nell'ambito europeo.

Ad oggi, l'Istituto di Calcolo e Reti ad Alte prestazioni del CNR e il Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica sono impegnati nell'attuazione del progetto "Evoluzione e Interoperabilità Tecnologica del Fascicolo Sanitario Elettronico" per portare su cloud servizi avanzati offerti dal FSE.

Nell'ambito di tale progetto si è svolta una analisi valutativa preliminare all'adozione del cloud per l'erogazione dei servizi del FSE, presentata in questo lavoro.

2. Aspetti fondamentali analizzati ai fini dell'adozione del Cloud per il FSE

In questa sezione è trattata l'analisi valutativa preliminare all'adozione del cloud per l'erogazione dei servizi del FSE. L'analisi condotta si è concentrata su cinque aspetti fondamentali:

- Aspetti economici

- Aspetti giuridici
- Aspetti di Privacy e sicurezza dei dati
- Aspetti tecnici implementativi

Ogni Regione e PA che intende adottare la tecnologia cloud deve attentamente considerare gli aspetti trattati in questo lavoro al fine rispettare le attuali normative di riferimento e minimizzare i rischi intrinseci in tale tecnologia.

2.1. Aspetti economici

L'economia ha un ruolo importante nel plasmare le trasformazioni di settore. Le attuali discussioni sul cloud si basano principalmente sulla complessità tecnica e sui problemi relativi all'adozione di questo ambiente. Sebbene l'esistenza e l'importanza di tali preoccupazioni siano innegabili, in genere gli aspetti economici di base hanno un impatto molto più forte sulla direzione e sulla velocità del cambiamento in quanto le sfide tecnologiche vengono risolte o superate attraverso il rapido processo di innovazione a cui ci siamo abituati.
L'arrivo dei servizi cloud cambia ancora una volta l'economia del settore informatico. La tecnologia cloud standardizza e raggruppa le risorse IT e automatizza molte delle attività di manutenzione attualmente eseguite manualmente. Le architetture cloud favoriscono scenari di utilizzo flessibile, self-service e forme di pagamento a consumo. L'ambiente cloud può produrre risparmi e altri benefici economici in almeno quattro aree:

- impatto a livello macro-economico
- risparmi da parte dei cloud provider
- aggregazione della domanda
- efficienza del multi-tenancy

Le possibilità di risparmi dovuti all'adozione del Cloud non deve portare a perdere di vista altri aspetti altrettanto importati come quello giuridico/normativo, di sicurezza e privacy, delle performance e tecnici implementativi trattati nei prossimi paragrafi.

2.2. Aspetti giuridici

Occorre evidenziare che non esistono attualmente delle disposizioni specifiche, nazionali o comunitarie, che disciplinino i contratti di cloud computing e che gli strumenti contrattuali attualmente proposti dai cloud provider appartengono prevalentemente alla categoria dei contratti c.d. "per adesione" nei quali, sostanzialmente, le clausole non sono negoziabili e sovente non definiscono aspetti assai delicati (ad es. responsabilità, livelli di servizio, legge applicabile, ecc.); si rischia quindi, di non garantire la necessaria coerenza alle disposizioni che disciplinano in Italia gli appalti pubblici.
Da una attenta analisi del contratto di cloud computing (nel rispetto delle esigenze di privacy e sicurezza dei dati secondo quanto espresso dal Garante della Privacy) [1], si ritiene che la sua qualificazione giuridica più "convincente" sia quella di un appalto di servizi disciplinato dalle disposizioni del codice civile applicabili anche in caso di appalti pubblici di servizi (come espressamente previsto dalle disposizioni del Codice degli appalti - D. Lgs. 163/2006).

Garanzie contrattuali

La formula contrattuale individuata (appalto di servizi) permette di inserire clausole contrattuali a tutela dell'ente pubblico che intende stipulare il contratto di cloud computing.
Per il controllo dell'erogazione dei servizi FSE è importante prevedere l'uso:

a) dei Service Level Agreement (SLA), con i quali si definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi (provider) nei confronti dei propri clienti/utenti

b) dei Privacy Level Agreement (PLA), con riferimento ai livelli/accordi/garanzie di tutela e sicurezza dei dati personali che il cloud provider si impegna a mantenere verso il cliente.

Oggetto dei PLA potranno essere :

- specifiche misure di sicurezza sui dati
- limiti nella circolazione/trasferimento dei dati, sia territoriali che con riferimento ai soggetti coinvolti
- esplicite garanzie con riferimento al mantenimento di un adeguato livello di tutela dei dati personali
- indicazione delle politiche di persistenza dei dati con riferimento alla loro conservazione (data retention)

Particolare attenzione va posta sui limiti nella circolarità anagrafica. Infatti il garante della Privacy pone vincoli stringenti:

"I dati sanitari documentati nel Fse/dossier non devono essere in alcun modo diffusi. La circolazione indiscriminata delle informazioni idonee a rivelare lo stato di salute è infatti vietata espressamente dal Codice (artt. 22, comma 8 e 23, comma 5, del Codice). La violazione di tale divieto configura un trattamento illecito di dati personali sanzionato penalmente (art. 167 del Codice). Anche il trasferimento all'estero 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)."[1]
Pertanto, i PLA dovranno contenere i vincoli di circolarità anagrafica come espressamente indicato dal Garante della Privacy.

2.3. Potenziali rischi per la sicurezza

Alcuni rischi per la sicurezza del cloud sono presenti anche in altre tipologie di outsourcing mentre altri sono legati a questa specifica modalità di erogazione. Tra le principali criticità/rischi che i CSC (cloud service consumer) devono affrontare si possono ricordare [7]:

Loss of governance: quando il cliente necessariamente cede il controllo al fornitore di una serie di aspetti che impattano le difese di sicurezza. Lock-in: al momento attuale il modo in cui si fruisce dei servizi cloud e l'immaturità o l'assenza di strumenti, standard e formati di dati interoperabili rende difficile migrare da un fornitore ad un altro.

Isolation failure: per ottenere le necessarie economie di scala il cloud provider deve mettere in comune le risorse tra più clienti e consentirne l'accesso per la sola parte di specifica competenza (isolation). Esiste quindi la possibilità che per un attacco o per un errore tale separazione venga meno compromettendo la riservatezza. Compliance risks: ci sono situazioni in cui la compliance a leggi e regolamenti non è possibile tramite soluzioni cloud. Inoltre può capitare che il fornitore non possa fornire evidenza della propria compliance o non permettere audit da parte del cliente.

Management interface compromise: l'accesso alle interfacce di gestione del public cloud da parte dei clienti deve necessariamente avvenire tramite Internet e fornisce un maggior controllo rispetto alle soluzioni di hosting. Tale capacità però comporta un aumentato rischio per il cliente nel caso di vulnerabilità e attacchi.

Data protection: il cloud computing presenta molti rischi relativi alla protezione del dato. Può essere difficile per il cliente controllare che i dati siano utilizzati legalmente. Il problema è esacerbato nel caso di cloud federati (con trasferimenti multipli di dati) e con l'ampliarsi delle catene di subfornitura.

Insecure or incomplete data deletion: quando viene fatta una richiesta di cancellare una risorsa, come spesso accade nei sistemi operativi, essa può essere rimossa ma non effettivamente distrutta e resa irrecuperabile. Tale situazione che include anche i casi di distruzione dei supporti fisici da dismettere e le copie di backup, è oggettivamente più complessa nel caso di ambienti cloud multi cliente che condividono hardware e software.

Malicious insider: i danni che il personale interno all'organizzazione fa quando adotta comportamenti illeciti, sono molto elevati anche se numericamente meno frequenti degli attacchi dall'esterno. Ci sono persone nell'organizzazione che ricoprono ruoli estremamente delicati, come ad esempio gli amministratori di sistema. Un fornitore (ed un cliente)

di servizi cloud non possono esimersi dal considerare questo rischio in tutte le sue implicazioni.

2.4. Potenziali vantaggi per la sicurezza

Come evidenziato da analisi condotte da ENISA [7], il modello cloud è in grado di offrire alle organizzazioni pubbliche benefici dal punto di vista della sicurezza dovute in particolare a:

- specializzazione del personale e presenza di strutture dedicate che permettono soluzioni di sicurezza di maggior qualità rispetto a quelle consuete;
- migliori soluzioni per la business continuity e disaster recovery (ridondanza geografica, edge networks, riallocazione dinamica delle risorse, tolleranza ad attacchi, etc);
- maggiore efficienza ed efficacia nei processi di change management, patch management, hardening, incident management, security assessment e security testing.

Non bisogna dimenticare, infatti, che la sicurezza in ambito cloud deve essere valutata in relazione alle soluzioni che i clienti di servizi cloud avrebbero potuto realizzare al proprio interno con le risorse a loro disposizione. Infatti i CSP, potendo fare leva sulle economie di scala, sono in grado di realizzare soluzioni molto più evolute rispetto a quelle che sono, di norma, implementabili dai CSC su una molteplicità di realizzazioni di minori dimensioni.
Le caratteristiche delle soluzioni cloud possono, ad esempio, consentire di:

- realizzare architetture ridondate e geograficamente distribuite;
- scalare risorse per rispondere a eventuali attacchi di tipo DDoS;
- utilizzare servizi di monitoraggio evoluti; ridurre i tempi di reazione agli incidenti;
- realizzare soluzioni di sicurezza fisica più robuste;
- integrare l'organizzazione della sicurezza nei CERT e con le forze di polizia;
- assicurare maggiore omogeneità e coerenza delle varie soluzioni di sicurezza.

Infine, quando i CSP orientano i propri servizi verso modalità di erogazione standard e aperte ciò comporta, dal punto di vista della sicurezza, una tendenza a convergere su soluzioni di carattere analogo, con indubbi riflessi positivi sulle capacità di controllo ed esecuzione.

2.5. Dati da migrare su cloud

Nel trattamento di dati sensibili, come quelli sanitari del FSE, è importante considerare le norme disponibili in materia. Nelle linee guida del Garante della privacy in tema di FSE [1] si precisa che:

a) *"All'interessato deve essere consentito di scegliere, in piena libertà, se far costituire o meno un Fse/dossier con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti."*

Inoltre:

b) *"La titolarità del trattamento dei dati personali effettuato tramite il Fse/dossier deve essere di regola riconosciuta alla struttura o organismo sanitario inteso nel suo complesso e presso cui sono state redatte le informazioni sanitarie (es. azienda sanitaria o ospedale) (artt. 4 e 28, comma 1, lett. f) del Codice)."*

Nel rispetto delle indicazioni del Garante, all'atto della creazione delle informazioni, queste devono essere memorizzate presso l'organizzazione che le ha prodotte. Nel caso l'interessato dia il consenso affinché il dato prodotto possa costituire base storica per il FSE quest'ultimo potrebbe essere memorizzato su cloud con opportuni livelli di sicurezza e privacy adottati per il trasferimento delle informazioni.
Inoltre, secondo la b), è necessario che l'organizzazione che ha redatto le informazioni continui ad essere titolare del trattamento dei dati personali. Nella circostanza il cloud provider può rivestire il ruolo di responsabile esterno al trattamento dei dati.

L'informativa, da formulare con linguaggio chiaro da parte del titolare del trattamento dei dati, deve indicare tutti gli elementi richiesti dall'art. 13 del Codice in materia di protezione dei dati personali, oltre all'indicazione che i dati saranno trattati in un contesto di cloud con una sintetica esposizione delle caratteristiche di tale tecnologia.

Disaccoppiamento dei dati sanitari da quelli personali

Come specificato nell'art. 22 del Codice in materia di dati Personali [8] e ribadito nelle linee guida [1]:

"Devono essere, inoltre, assicurate: l'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;"

Per consentire un ulteriore livello di separazione dei dati e nel rispetto di quelle che sono le indicazione del Garante è consigliato separare quelle che sono le meta informazioni dalle informazioni complete contenute nei documenti. Pertanto, si può prevedere uno scenario architetturale in cui su cloud sono memorizzate solo le meta-informazioni che consentono la ricerca e localizzazione dei documenti e memorizzare le informazioni complete su infrastrutture tecnologiche residenti presso le ASL/AO che hanno prodotto le informazioni.
Per quanto riguarda la separazione dei dati personali da quelli sensibili è possibile utilizzare codifiche univoche del paziente che non consentono il collegamento diretto del soggetto con le informazioni sanitarie memorizzate su cloud. (come previsto anche dal DL Crescita 2.0 [9])
Se si prevede di cifrare i dati memorizzati presso le ASL/AO, allora è possibile ipotizzare anche lo scenario in cui tali dati possono essere memorizzati su cloud. In questo ultimo caso gli enti risparmierebbero sicuramente molte risorse economiche e potrebbero predisporre un unico sistema o virtualizzare i vari sistemi nel Cloud controllando l'intero processo di generazione e conservazione dei dati a livello centrale (Regionale). E' da sottolineare che in ottemperanza a quelle che sono le linee guida del Garante[1], punto a) del precedente paragrafo, è necessario mantenere una infrastruttura di memorizzazione a livello locale per memorizzare tutti quei documenti che i vari pazienti decidono di non far confluire nel proprio FSE.

2.6. Aspetti tecnici implementativi

In questo paragrafo sono tratti aspetti tecnici e scelte architetturali considerando l'ambito di applicazione della tecnologia cloud al settore dell'e-heath.

Modello di dispiegamento

La scelta del modello di dispiegamento da adottare è essenzialmente legata alla necessità di sovranità e controllo sui dati. Considerando il contesto dell'e-health dove i dati risultano sensibili è necessaria una particolare attenzione alla gestione degli stessi e un controllo assoluto su di essi. Inoltre è necessario ricercare un meccanismo di separazione tra i dati personali e quelli utili a rilevare lo stato di salute del soggetto come specificato nelle linee guida del garante della privacy [1].
Pertanto, si consiglia di utilizzare "Private Cloud" oppure considerare la possibilità di un "Community Cloud" che potrebbe risultare una scelta vincente in quanto le Regioni e le P.A. condividono l'obiettivo comune della cura e assistenza ai cittadini.

Modello di servizio

Considerando i risultati del censimento [6] condotto dal CNR relativo alla disponibilità di infrastrutture tecnologiche disponibili di FSE, si evince che molte Regioni hanno già sviluppato le loro soluzioni di FSE con tecnologie eterogenee. Per tutelare gli investimenti già effettuati e non legarsi a tecnologie specifiche, si consiglia di utilizzare un modello di servizio di tipo IAAS. Questo consente alle Regioni di garantirsi una maggiore flessibilità legata al minore accoppiamento tra cloud Provider e software utilizzato per la realizzazione del Fascicolo Sanitario Elettronico. Inoltre, questa scelta consente di tutelare gli investimenti già effettuati per la realizzazione della soluzione regionale di fascicolo sanitario elettronico, non comportando la modifica del software sviluppato installabile in un ambiente cloud di tipo IAAS.

3. Fascicolo Sanitario Elettronico su Cloud

Dall'analisi condotta nel precedente capitolo si evince che è possibile prevedere e predisporre su Cloud servizi di FSE. In questo capitolo si cerca di prevedere quelli che sono i possibili scenari di migrazione dei servizi FSE su cloud.

3.1. Panorama italiano

Dalla attività riguardante il censimento delle soluzioni di infrastrutture FSE esistenti a livello regionale/provinciale [6] condotta dal CNR, nell'ambito del progetto di ricerca "Salute in Rete", è emerso che la totalità dei sistemi di FSE è basata sul paradigma registry/repository.
I documenti sanitari digitali sono archiviati in repository siti presso le strutture sanitarie. Tali documenti vengono indicizzati in registry, localizzati presso i domini regionali, mediante la memorizzazione di opportuni metadati. Ogni Regione ha realizzato tali sistemi adottando scelte architetturali e tecnologiche eterogenee. (Figura 1)

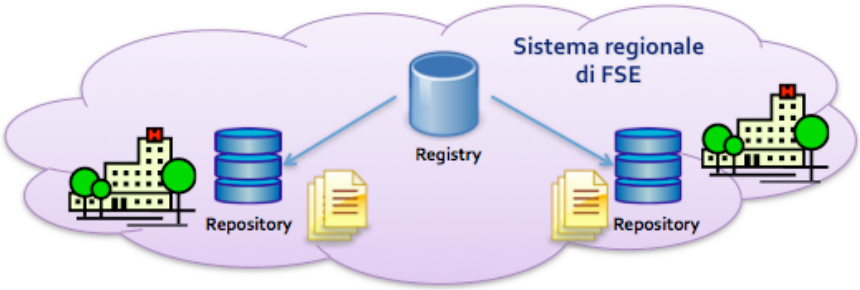

Figura 1 - Disposizione architetturale delle componenti FSE regionale

Considerando il dispiegamento delle componenti del FSE presso le infrastrutture tecnologiche dalle Regioni, InFSE assume un ruolo principale nel contesto dell'interoperabilità tra le soluzioni di FSE locali.
Come è mostrato in Figura 2, l'adozione di un modello di federazione dei registri prevede, per la ricerca e il recupero di un documento, un insieme di query federate che si propagano ai diversi livelli dei registri :

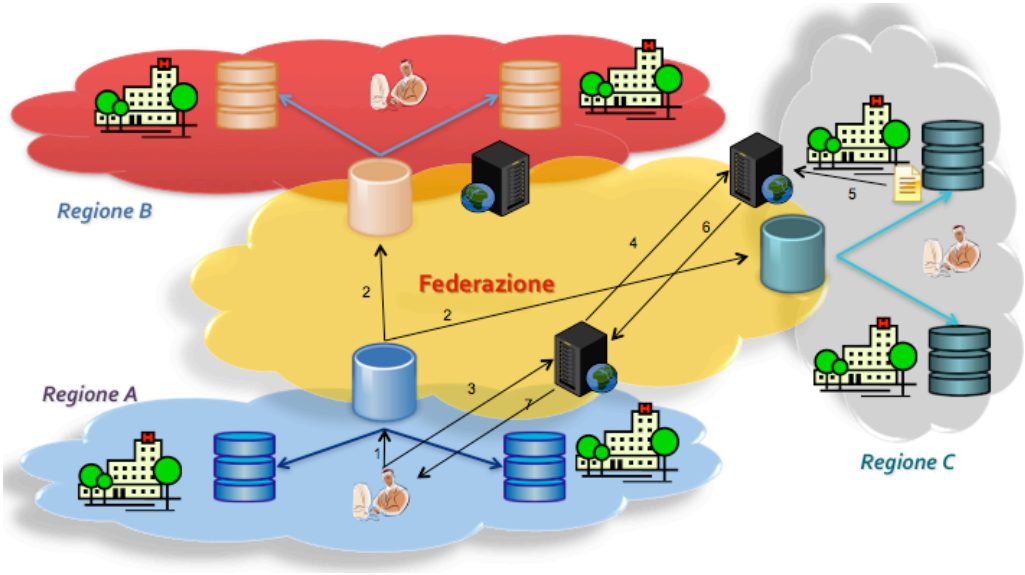

Figura 2 - Flusso di consultazione dei documenti nella modello InFSE

3.2. Fascicolo sanitario su Cloud

Considerando la possibilità di migrare tutte o in parte le componenti del FSE su cloud, in questo paragrafo si individuano i possibili scenari architetturali evidenziandone i pro e i contro per ognuno di essi.
Nel primo scenario Figura 3, ogni Regione/PA decide di appoggiarsi a Cloud Provider diversi e migrare solo le meta-informazioni (componente Registry Regionale) relative ai documenti memorizzati nei repository localizzati presso le strutture sanitarie. Il modello di servizio previsto è IASS e il modello di dispiegamento è Private Cloud per i motivi esposti nel paragrafo 3.4.2.

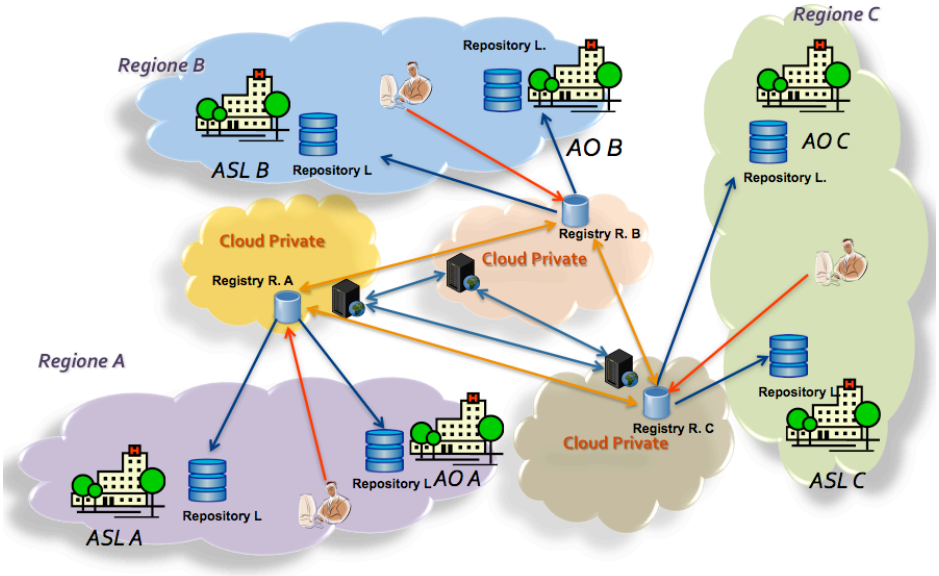

Figura 3 - FSE su cloud - primo scenario

Nel secondo scenario Figura 4, tutte le componenti del fascicolo sono migrate su cloud. È necessario comunque una componente "repository" presso gli enti che hanno prodotto l'informazione sanitaria, per i motivi esposti nel paragrafo 3.3.1 e l'adozione di tecniche di cifrature per tutti i dati memorizzati su cloud.

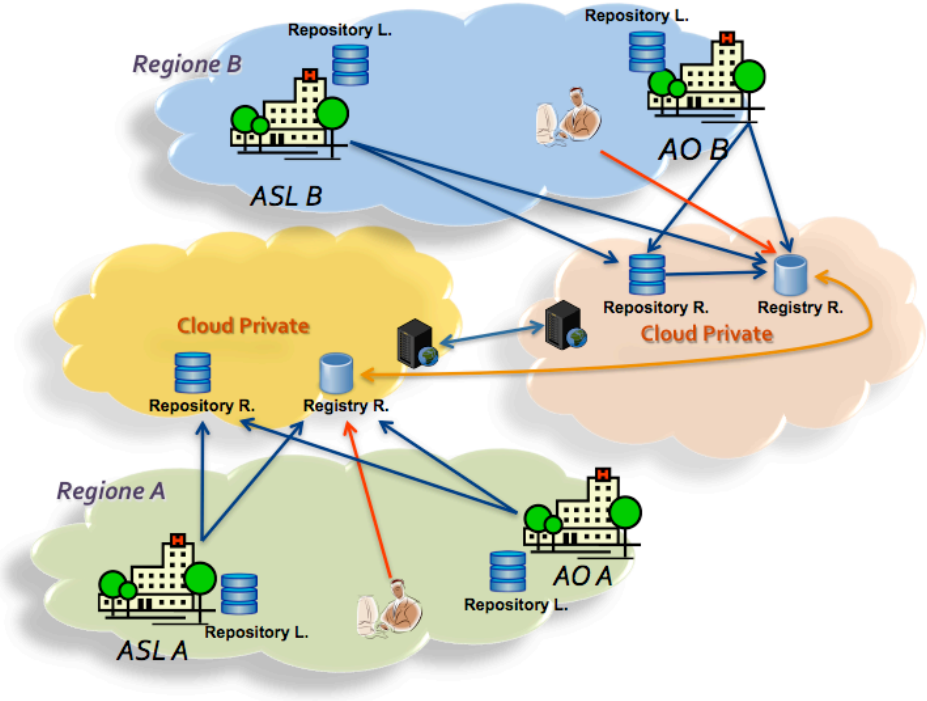

Figura 4 - FSE su cloud - secondo scenario

Nel terzo scenario Figura 5, si prevede la possibilità di adottare una dispiegamento delle componenti dei Fascicoli delle

diverse Regioni/PA su un Community Cloud.

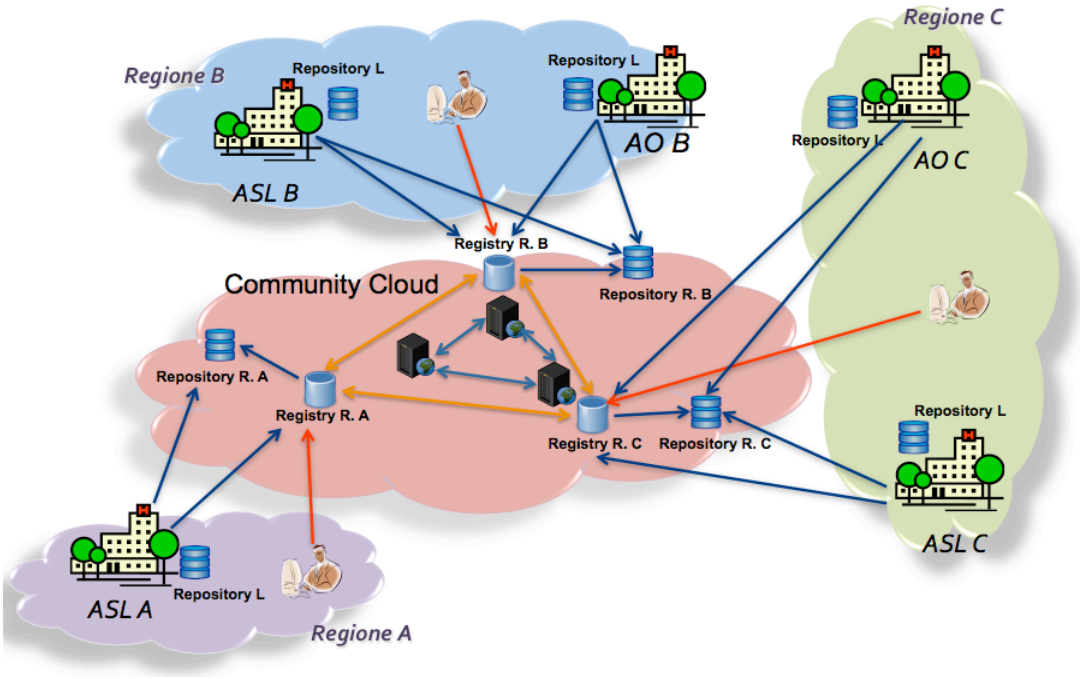

Figura 5 - FSE su cloud - terzo scenario

3.3. Pro e contro dei diversi scenari architetturali individuati

Nel primo scenario architetturale, che prevede il deployment delle componenti Registry su cloud mantenendo in locale i Repository dei documenti, si preserva il controllo assoluto sui dati da parte delle ASL/AO mantenendo tali informazioni in locale. Questo primo scenario che può sembrare vantaggioso per le ASL/AO in termini di controllo sui dati, può comportare una serie di problemi prestazionali, in quanto i repository nell'architettura potrebbero costituire un "collo di bottiglia" per l'accesso alle informazioni memorizzate sugli stessi Repository. Inoltre, per preservare il requisito di alta affidabilità del FSE, è necessario avere copie di recovery dei documenti, di conseguenza questa scelta prevede la predisposizione di una infrastruttura di memorizzazione ad alta affidabilità da parte dell'ASL/AO. Questo scenario è plausibile e giustificato solo quando le ASL o AO rappresentano grandi realtà, diventa difficilmente applicabile in "piccole" ASL che non dispongono di competenze interne e di risorse finanziarie sufficienti.
Nel caso di "piccole" strutture sanitarie sarebbe opportuno predisporre le componenti Repository e Registry su cloud (secondo scenario), garantendo in questo modo servizi di memorizzazioni con elevati standard di sicurezza e affidabilità. Anche le "grandi" ASL/AO potrebbero scegliere tale dispiegamento per massimizzare i risparmi portati dall'adozione del cloud.
La scelta del community cloud (terzo scenario) presuppone il perseguimento di uno scopo comune da parte dei soggetti che condividono tale scelta. Considerando il contesto del FSE, dove l'obiettivo comune è "la cura del paziente", è plausibile presupporre uno scenario "community cloud". È importante evidenziare che il risparmio enorme è dovuto alla forza di contrattazione che avrebbero le Regioni nei confronti di un unico Cloud Provider. La scelta del community cloud rappresenta una grande opportunità per le Regioni, ma è perseguibile solo se il percorso di innovazione è condiviso e gli obiettivi comuni sono posti al di sopra degli interessi specifici delle singole Regioni.
A seguire sono riportate le tabelle dove si evidenziano in maniera sintetica i pro e i contro per le soluzioni di dispiegamento adottabili (Private, Community, Public) e per gli scenari architetturali di dispiegamento individuati.

	Impatto economico	Impatto giuridico	Potenziali rischi per la sicurezza	Potenziali vantaggi per la sicurezza	Privacy dei dati
Public	🟢	🔴	🔴	🟢	🔴

Community					
Private					

Tabella 1 - Pro e contro dei modelli di dispiegamento

	Sicurezza	**Privacy dati**	**Prestazioni**	**Impatto economico**
1° scenario -Private cloud -Repository in locale -Registry su cloud				
2° scenario -Private cloud -Repository su cloud -Registry su cloud				
3° scenario -Community cloud -Repository su cloud -Registry su cloud				

Tabella 2 - Pro e contro degli scenari architetturali di dispiegamento individuati

4. Conclusioni

Dalle osservazioni svolte in questo documento si evince da subito quanto il cloud rappresenti una tecnologia particolarmente vantaggiosa per essere utilizzata nell'ambito di erogazione dei servizi del fascicolo sanitario elettronico, sia sotto il profilo del contenimento della spesa, sia sotto quello dell'efficienza, dell'interoperabilità e dell'implementazione di stringenti misure di sicurezza. È bene precisare, però, che nell'uso di questo tipo di tecnologia, è necessario un approccio pragmatico e prudente soprattutto per quanto riguarda la gestione e il controllo della sicurezza dei dati.

Le problematiche evidenziate, nell'adozione del cloud per l'erogazione dei servizi FSE, possono essere limitate o superate attraverso l'adozione di opportuni accorgimenti specifici di tipo tecnologico e/o contrattuali.

Rimane comunque l'urgenza di un intervento di carattere giuridico per permettere a tutti gli enti pubblici e alle grandi organizzazioni di usufruire a pieno delle enormi opportunità offerte dal paradigma cloud.

Riferimenti bibliografici

[1] Garante per la protezione dei dati personali - Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009.

[2] Garante per la protezione dei dati personali - Cloud computing: indicazioni per l'utilizzo consapevole dei servizi.

[3] Ministero della Salute - Il Fascicolo Sanitario Elettronico Linee guida nazionali - 11 novembre 2010.

[4] Raccomandazioni e proposte sull'utilizzo del cloud computing nella pubblica amministrazione, DigitPA, 28 giugno 2012.

[5] Infrastruttura tecnologica del Fascicolo Sanitario Elettronico - Linee guida, CNR, Luglio 2012.

[6] Infrastruttura tecnologica del Fascicolo Sanitario Elettronico -Fotografia commentata sperimentazioni esistenti su FSE, CNR, Dicembre 2010.

[7] Cloud Computing Security Risk Assessment, ENISA, November 2009.

[8] Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196.

[9] Decreto Legge 18 ottobre 2012, n. 179 (Crescita 2.0) convertito con la legge di conversione 17 dicembre 2012, n. 221, recante: «Ulteriori misure urgenti per la crescita del Paese.».

[10] Codice dell'Amministrazione Digitale - Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni.

[11] Cloud Computing - Benefits, risk and recommendations for information security, ENISA, Novembre 2009.

[12] NIST Cloud Computing Reference Architecture, September 2011.

[13] US Government Cloud Computing Technology Roadmap Volume I Release 1.00 (Draft). High- Priority Requirements to Further USG Agency Cloud Computing Adoption. NIST Cloud Computing Program Information Technology Laboratory, L. Badger, D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside and D. Leaf, November 2011.

[14] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, and P. Donzelli, "On Federating Health Information Systems", in GUT 2012: Proceedings of the International Conference in Green and Ubiquitous Technology, pp. 139-143, 2012, IEEE Press.

[15] C. Esposito, M. Ciampi, G. De Pietro, and P. Donzelli, "Notifying Medical Data in Health Information Systems", in DEBS 2012: Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems, pp. 373-374, 2012, ACM New York, NY, USA, ISBN: 978-1-4503-1315-5, DOI: 10.1145/2335484.233552.

[16] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, P. Mori, A. Gebrehiwot, and P. Donzelli, "On Securing Communications among Federated Health Information Systems", in SAFECOMP 2012 Workshops: Proceedings of the 31st International Conference on Computer Safety, Reliability and Security, Lecture Notes in Computer Science, vol. 7613, pp. 235-246, 2012, Springer-Verlag Berlin Heidelberg.

[17] G. De Pietro, A. Coronato, M. Ciampi, A. M. Urso, M. Cossentino, R. Rizzo, P. Storniolo, F. Folino, M. C. Buzzi, A. Gebrehiwot, "L'infrastruttura tecnologica del Fascicolo Sanitario Elettronico", I. Florio, M. T. Guaglianone (Eds.), Il Fascicolo Sanitario Elettronico: Infrastruttura tecnologica e codifica dei dati, pp. 85-127, 2012, CNR – SeGID, Collana Documentalia, ISBN: 978-88-906334-1-6, ISSN: 2239-8414 (Italian)

[18] G. De Pietro, R. Guarasci, M. Ciampi, A. M. Urso, M.C. Buzzi, C. Pizzuti, "L'interoperabilità nazionale del Fascicolo Sanitario Elettronico: il progetto InFSE", P. Tarallo (Ed.), Verso e-Health 2020, Il Sole 24 Ore Sanità, 2012, ISBN: 978-88-324-8172-3 (Italian)

[19] P. Donzelli, G. De Pietro, R. Guarasci, M. Ciampi, and M. T. Chiaravalloti, "Infrastruttura del Fascicolo Sanitario Elettronico: dalle regole alla realizzazione", e-HealthCare, Anno 4, Numero 20, Settembre – Ottobre 2012, pp. 16-22, Edisef, ISSN: 2038-4238 (Italian)