Requisiti dei Centri Servizi

Fulvio Glisenti

CO.ME.TE - Consorzio per la Ricerca, Sviluppo e Sperimentazione di Sistemi di Telemedicina, Health Telematic Network - Servizi di Telemedicina, Brescia

(G Ital Cardiol 2009; 10 (Suppl 1-1): 10S-13S)

Per la corrispondenza:

Dr. Fulvio Glisenti

CO.ME.TE - Consorzio per la Ricerca, Sviluppo e Sperimentazione di Sistemi di Telemedicina Health Telematic Network - Servizi di Telemedicina
Via Aldo Moro, 13
25124 Brescia
E-mail: fglisenti@e-htn.it

Un Centro Servizi di Telemedicina dovrebbe avere un prerequisito fondamentale: quello di essere organizzato come un *hub* che gestisce ingenti e continui flussi di dati sanitari sensibili in ingresso (segnali biologici, immagini, testi, suoni) e quindi, sostanzialmente, essere un *call/contact center* multimediale che eroga servizi in modalità ASP *(Application Service Provider)* da una piattaforma tecnologica *web-based*.

L'ASP è un aspetto evoluto dell'*outsourcing* in cui hardware e software non sono localizzati nella sede degli utilizzatori ma risiedono nella sede del fornitore del servizio. La modalità di erogazione ASP è indispensabile per avvalersi di servizi di elevato livello qualitativo senza doversi necessariamente dotare di strumenti e competenze onerose.

Come *hub* il Centro Servizi:

- organizza un *team* di risorse umane, tecnico-professionali (formate e dedicate);
- realizza un *network* di comunicazione tra diversi utenti: ospedali, strutture universitarie, medici specialisti, medici di medicina generale, pazienti-utenti;
- realizza *flow-chart* operative di monitoraggio degli utenti;
- gestisce un database di dati sensibili;
- gestisce la sicurezza con la protezione dei dati sensibili attraverso l'elaborazione di severi documenti programmatici sulla sicurezza, e con la registrazione delle conversazioni professionali;
- garantisce la qualità certificata UNI EN ISO 9001/2000;
- supporta la ricerca scientifica;
- gestisce ed organizza il telelavoro delle figure professionali coinvolte essendo l'obiettivo quello di "remotizzare" il più possibile la parte professionale (cardiologi, *nursing* e *triage* infermieristici) in modo da rendere flessibile il sistema rispetto alle chiamate in ingresso e quindi facilmente scalabile il traffico in entrata; tecnologicamente deve poter rendere usufruibili dalla piattaforma multimediale modalità di telelavoro via web.

I sistemi di telemedicina del Centro Servizi dovrebbero essere in grado di:

- comunicare con altri sistemi analoghi al fine di garantire l'interoperabilità fra centri diversi;
- comunicare con tutti i sistemi informativi sanitari istituzionali.

Il Centro Servizi deve avere la possibilità di integrare nel database i segnali biologici, trasmessi in formato analogico o digitale, provenienti dai dispositivi delle principali aziende presenti sul mercato.

La piattaforma tecnologica multimediale *web-based*

Gli elementi cardine dell'infrastruttura tecnologica, il cui funzionamento va protetto da adeguati gruppi di continuità, dovrebbero sinteticamente essere:

- la rete di *back-end*
- la rete di *front-end*
- la connettività
- il *firewall* per la sicurezza dati
- il sistema CTI *(Computer-Telephony Integration)*
- le postazioni di lavoro in rete
- gli applicativi clinico-gestionali
- i *service level agreement* (SLA)
- l'*help desk*.

Rete di back-end

Il Centro Servizi deve potersi avvalere di una serie di server idonei a svolgere funzioni separate ma integrate per rispettare quei vincoli di sicurezza e continuità del servizio necessari alla realizzazione di una soluzione *mission critical*.

I componenti critici della struttura devono essere costituiti da macchine con componenti ridondanti (soluzioni raid, doppi alimentatori) o meglio ancora in soluzione *cluster*. La ridondanza degli elementi hardware utilizzati determina un elevato valore di HA *(High Availability)*, elemento che contraddistingue quelle risorse impiegate in applicazioni e soluzioni *mission critical*.

Per *back-end* si intende la rete sulla quale si attestano i sistemi che implementano la logica applicativa del servizio. Alla base degli applicativi sviluppati per la gestione della scheda sanitaria deve essere presente un server opportunamente dimensionato per ospitare un RDBMS *(Relational Database Management System)*. Sul sistema sono presenti database separati che consentono la memorizzazione dei dati clinici e dei dati amministrativi gestionali.

L'architettura consente ai PC remoti di operare contemporaneamente sia come *thin client* che come *client* tradizionali. La tecnologia di *back-end* consente di trasmettere al *client* solo l'interfaccia utente grafica (GUI, *Graphical User Interface*) dell'applicazione; in questo modo i dati non vengono mai trasferiti in rete escludendo quindi anche la possibilità di intercettazione degli stessi da parte di terzi non autorizzati. Ciascun utente che si connette visualizza solo la propria sessione che viene gestita in modo trasparente dal sistema operativo server ed è indipendente da qualsiasi altra sessione *client*. Ogni operatore che svolge attività al Centro Servizi riceve in dotazione utenze personalizzate con le quali ha la possibilità di accedere ai vari applicativi; l'uso esclusivo e personale di tali parametri rende semplice il tracciamento di tutte le operazioni che avvengono sui sistemi interni. L'implementazione quindi di profili comuni e di *group policy* restrittive limita, di fatto, l'utilizzo dei sistemi *client* da parte degli operatori del *call center* alle sole aree necessarie allo svolgimento della loro attività.

Il centro deve avvalersi di un sistema di posta elettronica o di altri mezzi di comunicazione (SMS, fax, ecc.) che consentano un efficace e rapido scambio di informazioni con gli utenti.

Rete di front-end

La rete di *front-end* è quella su cui vengono localizzati i sistemi che attuano servizi direttamente a contatto con l'utente o con la rete di trasporto pubblica.

L'esposizione ad Internet è filtrata da un *backbone firewall* rendendo in questo modo sicura la rete di *back-end* già descritta.

Il modulo software per la gestione e la consultazione è raggiungibile attraverso un *browser* su rete Internet. Il sistema di accesso deve poter essere gestito attraverso l'attivazione di profili utente che determinino le operazioni eseguibili. Il requisito può essere soddisfatto secondo un modello che operi con un'autenticazione a fattore multiplo.

A seguito di un primo livello di autenticazione basato su *login/password*, l'utente deve inserire una seconda credenziale, basata però sul modello *One Time Password* (OTP), per accedere al sistema: una OTP consiste in una password che non è fissa, ma è dotata di un periodo temporale di validità e cambia ogni volta che si accede al sistema.

L'utente può venire a conoscenza di questa seconda password tramite:

- l'utilizzo di dispositivi hardware per la generazione di *token* basati su algoritmi non reversibili (ad es. apparati in uso in alcuni sistemi di *home banking*);
- l'invio via SMS (dato il forte disaccoppiamento tra i canali web/sms si ritiene sicuro operare secondo questa modalità).

Con il meccanismo OTP si raggiunge un elevato grado di sicurezza per il requisito di autenticazione. A seconda del tipo di profilo abilitato, si ha un diverso livello di accesso alle varie aree che compongono i database clinico-amministrativi (sola lettura, lettura/modifica, lettura/modifica/cancellazione, ecc.).

Quando un *client* si colleghi via https (con un qualunque *browser*), il sistema deve processare le richieste che arrivano dal *client* (dalla richiesta iniziale di *login*) e predisporre le pagine html opportune da rendere visibili al *client* come risposta alla richiesta ed in base agli algoritmi di accesso ai dati, propri del motore web. Il *client* deve quindi procedere ad una semplice navigazione attraverso pagine html opportunamente predisposte, mentre l'intera elaborazione risiede sul server.

Connettività del Centro Servizi

Il Centro Servizi dovrebbe avvalersi almeno di una doppia connessione in banda larga (ad es. di tipo xDSL con 2-4 mbit/s), di cui una con funzioni di back-up, che consenta il collegamento da e verso i suoi utenti. La linea di back-up può essere utilizzata anche per la gestione di picchi di traffico attraverso una soluzione software di bilanciamento del traffico *(load balancing)*. La soluzione garantisce in questo modo un elevato standard di funzionamento aumentando sensibilmente la qualità e la continuità del servizio. Non dovrebbero essere escluse *a priori*, per talune applicazioni, le opportunità di utilizzo di connessioni satellitari, UMTS *(Universal Mobile Telecommunications System)* e *wireless*.

Firewall per la sicurezza dati

Uno degli aspetti più critici nel panorama tecnologico degli ultimi anni è rappresentato dalla sicurezza informatica. Il rischio di violazione dei sistemi sempre in linea (in relazione alle connessioni *always-on*) è di rilevanza tale da aver motivato una specifica raccomandazione di intervento delle Autorità competenti [ricorso a VPN *(Virtual Private Network)*, crittografia]. Si raccomandano pertanto livelli di *firewalling* diversificati per consentire l'accesso ai software attraverso connessioni protette.

La tecnologia VPN sfrutta la connessione alla rete pubblica (Internet) delle postazioni remote offrendo la possibilità di collegarsi ai sistemi di *back-end* in modo totalmente sicuro. Questo grazie all'instaurarsi di un canale di comunicazione (tunnel) reso inattaccabile da terzi tramite la criptazione dei dati che il tunnel trasporta.

Un VPN *Gateway* garantisce sicurezza assoluta nell'ambito delle connessioni remote; tale garanzia è data dal metodo di criptazione dei dati ad alto rendimento che l'apparato offre. La possibilità inoltre di stabilire il tunnel VPN con l'ausilio di apparati hardware può essere una valida alternativa dove richiesto dalle condizioni di utilizzo del servizio (ad es. sedi remote con un numero elevato di connessioni contemporanee). La centralizzazione della configurazione dell'apparato rende più semplice ed immediata la gestione di tutto il sistema di connessione.

Questa tecnica garantisce la riservatezza e la sicurezza delle comunicazioni grazie al fatto che i dati duranti il passaggio vengono criptati adeguatamente e quindi resi illeggibili da eventuali malintenzionati che intendessero intercettarli. La soluzione è in grado di offrire un collegamento stabile e sicuro attraverso l'utilizzo di apparati hardware che determinano la realizzazione di tunnel *site to site* sulla rete pubblica. Il VPN *Firewall* determina un livello di fil-

tro in grado di impedire qualsiasi accesso ai sistemi di *back-end* se non autorizzati dal VPN *Gateway* integrato.

Sistema CTI (Computer-Telephony Integration)

Il sistema CTI deve essere un ambiente integrato per la gestione degli strumenti di comunicazione dai più tradizionali (telefono e fax) a quelli tecnologicamente più avanzati (web, e-mail, IP *Telephony*). Quindi una piattaforma che comprenda in un unico ambiente tutte le funzionalità che l'approccio tradizionale propone come composizione di singole soluzioni proprietarie con funzioni specifiche (PBX, ACD, IVR, ecc.).

Il sistema deve consentire:

- la gestione dei diversi sistemi di comunicazione aziendale (PBX, IVR, ACD, e-mail, fax);
- l'integrazione con sistemi di *workflow* e con applicazioni verticali specifiche;
- l'interazione con database interni ed esterni (RDBMS, OLAP);
- l'integrazione con servizi Internet per lo svolgimento di attività di *Web Call Center*;
- transazioni di *unified messaging*;
- gestione di conversazioni telefoniche a più interlocutori *(conference calls)*.

Le funzioni sono fruibili da parte degli operatori del Centro Servizi attraverso l'utilizzo del software *client* presente sulle loro postazioni, in particolare il software deve consentire di:

- intercettare la chiamata in ingresso;
- accogliere l'utente con un messaggio di benvenuto che richiami l'attenzione sulla procedura di registrazione della conversazione.

La chiamata deve poter essere inoltrata alla prima postazione libera, dove l'operatore, determinato il motivo del contatto, rende possibile l'attivazione di una conferenza a tre con lo specialista interessato. L'operatore deve inoltre essere in grado di stabilire se lo specialista è già impegnato in una conversazione precedente nel *client* presente sulla propria postazione che visualizza lo stato degli specialisti in quel momento (libero, occupato).

Il Centro Servizi deve essere attestato su un flusso primario ed eventualmente su un unico Numero Verde al quale ogni paziente/utente può fare riferimento. La presenza di alcuni numeri d'emergenza alternativi al flusso digitale rappresenta un ulteriore elemento per aumentare il valore di HA determinante nelle soluzioni *mission critical*.

Postazioni call center

Sono le postazioni dalle quali gli operatori del Centro Servizi devono poter gestire il flusso delle informazioni del paziente. Grazie all'utilizzo di group policy specifiche ogni *client* mostra agli operatori un *desk top* comune, non modificabile da parte degli utenti e contenente le applicazioni specifiche del servizio.

Di seguito sono sintetizzate le funzionalità e i servizi all'interno del *call center*:

- postazioni di lavoro. Sono le postazioni dalle quali gli operatori del *call center* gestiscono il flusso delle informazioni dell'utente. Sulle postazioni è presente un applicativo *client* che è connesso al database centrale; chi opera sulla postazione è in grado di svolgere tutte le attività che la scheda sanitaria offre;
- CTI. È la centrale telefonica che con l'ausilio di applicativi *custom* è in grado di velocizzare lo smistamento delle chiamate verso le postazioni di lavoro. La centrale inoltre registra le conversazioni telefoniche che avvengono nel *call center*;
- file server. Il *file server* gestisce tutte le operazioni di *office automation* che sono proprie di una rete LAN locale. Alcuni dei servizi svolti da questo apparato sono: 1) *mail server*; 2) *fax server*; 3) *file share*: archiviazione centralizzata dei documenti.

Applicativi clinico-gestionali

Il corretto tracciamento delle informazioni acquisite attraverso i contatti tra pazienti, ospedali e Centro Servizi deve essere assicurato dall'utilizzo di un applicativo clinico. I *tools software* da sviluppare ed utilizzare costituiscono un set di strumenti integrati per la gestione di dati clinici e amministrativi nonché eventualmente di protocolli di ricerca sperimentali; devono essere realizzati in modo da risultare compatibili/interoperabili con altre piattaforme e database relazionali; idealmente dovrebbero essere in grado di operare con duplice modalità *client/server* oppure attraverso l'utilizzo dell'interfaccia web realizzata per operare in modo remoto.

L'integrazione delle funzioni in un unico ambiente, l'aiuto in linea e l'aderenza agli standard CUA *(Common User Access)* riducono al minimo l'esigenza di una formazione specifica.

La struttura dei dati contenuta nella scheda sanitaria dovrebbe essere organizzata in moduli, eventi, contenenti sottoinsiemi di informazioni omogenee (anagrafica, posizione amministrativa, anamnesi, esame obiettivo, esami strumentali, terapia, dati infermieristici, contatto telefonico, visite specialistiche, ecc.) replicabili nel tempo.

L'applicativo deve permettere di gestire in modo integrato immagini e dati, a video e su stampa, scegliendo gli schemi di *reporting* più adatti ad una migliore interpretazione delle informazioni.

Per un efficace controllo degli errori di *data entry*, devono essere definite procedure di verifica sulle caratteristiche e la validità dei dati introdotti. I campi dati devono essere di vario tipo (testo, numerici, data, a risposta predefinita, ecc.) e per ognuno di loro devono essere definibili specifici controlli. I dati contenuti nelle "schede paziente" devono poter essere estratti seguendo schemi e formati diversi, in accordo con regole di selezione predefinite, per il trasferimento ad altri programmi (post-elaborazione, statistica, grafica) consentendo così l'estrazione dei tracciati *record* previsti da protocolli istituzionali. Il database utilizzato deve essere compatibile con gli standard di mercato in modo da garantire sviluppi indipendenti dall'applicativo e rapidi/facili trasferimenti *import/export* di dati da/verso altre applicazioni, ovvero integrati, ad esempio con piattaforme regionali. Ogni utente abilitato all'utilizzo dell'applicativo deve ricevere utenze personalizzate che dovranno essere impiegate per l'autenticazione iniziale. I codici generati sono assolutamente riservati e vengono utilizzati per il tracciamento delle attività svolte sulle diverse postazioni di lavoro.

SLA, assistenza e manutenzione

Il Centro Servizi deve essere attivo h24/365 giorni all'anno

con un numero massimo definito e programmato di interruzioni del servizio a scopo di manutenzione preventiva. Gli interventi devono essere comunicati con un congruo anticipo. Devono inoltre essere garantiti:

- tempi di permanenza in coda non superiori ai 30 s per l'80% delle chiamate entranti;
- tempi di permanenza in coda non superiori a 50 s per il restante 20% delle chiamate entranti;
- le percentuali suddette sono da calcolarsi su tutte le chiamate in ingresso eccetto quelle abbandonate entro 30 s (tali valori rappresentano standard di mercato per attività di *call center* con carichi giornalieri superiori a 100 chimate/giorno);
- registrazione delle conversazioni;
- rendicontazione evolutiva delle chiamate (numero, durata, provenienza, ecc.).

Help desk

In caso di malfunzionamento del servizio o delle apparecchiature il Centro Servizi deve garantire, attraverso un *help desk* h24, adeguati e definiti livelli di assistenza correttiva con una precisa definizione dei gradi di severità del disservizio:

- alta: disservizio e/o malfunzionamento che comporta un blocco totale del sistema che determina il blocco delle attività;
- media: disservizio e/o malfunzionamento che comporta un blocco parziale del sistema con forte degradazione delle prestazioni;
- bassa: disservizio e/o malfunzionamento che comporta un errore di sistema con conseguente degradazione minore delle prestazioni, e non bloccanti per le attività.

Tempi di intervento per l'assistenza sistemistica, di *networking* ed applicativa: per guasti a severità alta entro il giorno lavorativo stesso, per guasti a severità media entro il giorno lavorativo successivo, per guasti a severità bassa controllo da remoto delle apparecchiature per la verifica del funzionamento ottimale delle stesse.