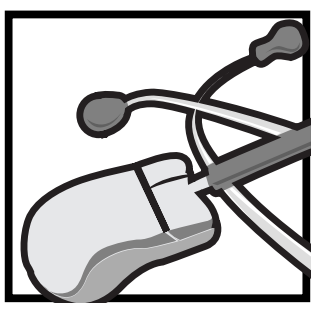


Per i programmi utilizzati nell'assistenza sanitaria sono insufficienti le marcature Ce ma

Ict: meno rischi clinici con un

L'esperienza condotta agli Ospedali Riuniti di Bergamo ha dimostrato la

Il proposito di questo articolo è aprire un dibattito sull'adozione di una condivisa metodologia di analisi del rischio e di una adeguata certificazione di qualità, per i prodotti software da utilizzare nella pratica clinica. Va premesso che la riflessione nasce da esperienze operative svolte "sul campo", con l'impiego di strumenti software dedicati alla specifica attività di medici e infermieri.

La tipologia di software di cui stiamo parlando è ancor oggi relativamente poco diffusa nelle corsie dei nostri ospedali, e conseguentemente il dibattito è da considerarsi ai suoi albori.

Recentemente, tuttavia, è intervenuto un evento che pone all'ordine del giorno questo tema, vale a dire la variazione della normativa comunitaria che include il "software" in quanto tale nelle categorie di oggetti definiti «dispositivi medici». Chiunque abbia un po' di dimestichezza con le apparecchiature sanitarie, avrà sentito parlare della "marcatura Ce", obbligatoria appunto per gli oggetti qualificati come «dispositivi medici». In termini molto semplificati, possiamo dire che un oggetto tecnologico è un «dispositivo medico» se il produttore dichiara che tale è la sua destinazione d'uso, e opera di conseguenza per ottenere la relativa certificazione, secondo le modalità previste dalle norme. Ne consegue che nessun medico accetterebbe di utilizzare un ecografo o una Tac sprovvisti del "bollino Ce", mentre lo stesso medico probabilmente non si è mai posto la questione di un'analoga certificazione per gli strumenti software.

La nuova normativa, paradossalmente, apre uno scenario problematico per il sanitario, perché la sua applicazione acritica rischia, da un lato, di rallentare l'evoluzione possibile degli strumenti software a supporto della pratica clinica e, dall'altro, di indurre un falso senso di sicurezza - quasi che bastasse l'apposizione di questo marchio in un angolo dello schermo di un computer a garantire la sicurezza di una procedura clinica.

La tesi di questo articolo è che - in ambito ospedaliero - abbiamo a che fare con "sistemi" organizzativi e informativi di elevata complessità, per i quali le pur rigorose previsioni di certificazione "Ce" sono insufficienti, e che richiedono invece di pensare a modalità di "certificazione" più adeguate alle caratteristiche loro proprie.

Possiamo definire queste caratteristiche in rapporto a quelle più comuni di un generico dispositivo medico. Di quest'ultimo, a esempio, si può sostenere che: è sottoposto a certificazione e a taratura; è "sigillato"; è brevettato (è un sistema proprietario); è un prodotto di (piccola/media) serie; ha un utilizzo procedurale (protocolli - manuali di istruzione); è sostituibile, vale a dire può essere messo "off line", oppure duplicato, oppure surrogato con altro strumento; infine, non prevede (di norma) utilizzi simultanei da parte di una pluralità di operatori. Se ne può concludere che stiamo parlando di oggetti che sono realizzati e utilizzati come "scatole nere", e nei quali tutti gli sforzi di progettazione sono rivolti a predefinire le modalità di interazione con l'essere umano e con altre componenti tecnologiche.

Al contrario un software gestionale o di proces-

La procedura per la certificazione del software è stata messa a punto, inizialmente, a partire dall'esperienza maturata con la messa in produzione di un sistema informatizzato di gestione della Terapia farmacologica e, successivamente, con la sua applicazione ad altri ambiti critici (procedura di richiesta da reparto degli emocomponenti).

La prima esperienza riguarda un sistema informatizzato per la gestione della terapia farmacologica per i pazienti ricoverati, presso gli Ospedali riuniti di Bergamo a partire da maggio 2006 (v. tabella).

Dalla prima versione, nella quale erano presenti alcune funzioni base per l'oncologia e l'ematologia, si è passati a un sistema correntemente utilizzato in circa 25 realtà mediche differenti. L'aumento delle funzioni e della complessità del processo operativo che il sistema gestisce, ha portato alla necessità di un controllo sulla sua sicurezza e affidabilità, considerando che le azioni e gli elementi su cui si lavora sono collegati alla salute del paziente.

Nel 2007 si è proceduto a un test estensivo del sistema per individuarne eventuali difetti, anomalie e problemi che lo strumento, se non correttamente pensato e utilizzato, può causare al paziente. Gli elementi su cui è stato sviluppato il lavoro sono i documenti di specifica redatti in azienda a seguito delle interviste sul campo con i futuri utenti e utilizzati dopo per lo sviluppo del software e i documenti operativi prodotti durante l'avviamento e l'utilizzo quotidiano del sistema.

I malfunzionamenti generano gli errori

Per approssimazioni e revisioni successive, utilizzando sia metodologie consolidate nel campo del "software engineering", sia approcci innovativi più avanti descritti, sono stati realizzati ed eseguiti circa 2.900 casi di prova. Poi il sistema è stato perfezionato nei punti individuati dal test. Nel corso dei lavori è apparsa sempre più evidente la necessità di considerare due diversi aspetti del percorso di certificazione: considerare l'affidabilità del prodotto, legata a tutte le funzionalità messe a disposizione dal prodotto software, ma anche condurre un'analisi di rischio legata all'utilizzo dello strumento. Questo secondo aspetto pone il problema se un insieme di funzioni separate ma tra loro collegate nel processo operativo possono originare, da un problema di una, effetti critici sul percorso completo di terapia per il paziente.

Aspetti metodologici. Il metodo che abbiamo seguito per condurre le attività di verifica e analisi sopra descritte tiene conto degli aspetti di contesto in cui ci si pone: l'utente è un acquirente e utilizzatore di software per uso clinico, tipicamente un ente ospedaliero; il software può essere stato sviluppato ad hoc per l'ente oppure può essere un prodotto acquisito in licenza d'uso; il prodotto acquisito può anche essere estensivamente parametrizzato in modo che il suo comportamento reale, una volta installato, non dipenderà solamente dal programma, ma anche dallo stato dei parametri di configurazione.

Conseguentemente il metodo si compone di tre approcci differenziati per livello: il livello dell'interazione sistemica (Fmea; modalità di rilascio e attivazione del prodotto); il livello dell'analisi funzionale (eseguito in condizioni "di laboratorio"); il livello della "safety" (eseguito in condizioni che simulano l'operatività).

Il primo aspetto metodologico è di fondamentale importanza. Un'applicazione software per uso clinico è parte di un sistema informativo più ampio ed è soggetta a evoluzione nel tempo. L'applicazione può essere modificata e adattata a nuove regole organizzative ed esigenze, o interfacciata con altre applicazioni, o modificata funzionalmente, a esempio adattandone i parametri di configurazione. Questa evoluzione può portare a delle variazioni nell'affidabilità e nella sicurezza d'uso e rendere non più significative le pur rigorose verifiche effettuate "in laboratorio", prima del suo effettivo utilizzo "in produzione". È quindi di essenziale importanza che il processo di gestione dell'applicazione sia accuratamente specificato e posto sotto controllo. Si pensi a esempio alla seguente sequenza di eventi: è identificato un malfunzionamento, il software è corretto ed è generata una nuova versione, per errore è messa in produzione la versione precedente, oppure il personale non è correttamente informato e non utilizza la funzionalità rilasciata. Ogni modifica deve perciò essere autorizzata, gestita e tracciata, il rilascio in produzione di una nuova versione deve essere controllato e per ogni modifica deve essere riconsiderata la valutazione di sicurezza d'uso al fine di decidere se è necessario rivederla o estenderla. Si noti che questo processo deve definire con precisione tutti i componenti che vanno messi sotto controllo, sia tecnologici che organizzativi. Un esempio significativo è la presenza di dati attraverso i quali è possibile configurare un prodotto software acquisito in licenza da un produttore. In questo caso il sistema è composto dal software e dai dati di configurazione ed entrambi devono essere considerati in un processo unitario di gestione. L'interazione tra persone e sistema, infine, mette in evidenza elementi problematici: dall'analisi formale (Fmea) si ricavano indicazioni su dove sia meglio inserire controlli e ausili all'operatività umana (messaggi di avvertimento; blocchi all'esecuzione di procedure non corrette).

Preliminarmente tuttavia, l'obiettivo è raggiungere una ragionevole garanzia sulla "qualità" del prodotto. In particolare, consideriamo due specifici aspetti: l'affidabilità (la proprietà di comportarsi come specificato, senza malfunzionamenti) e la sicurezza d'uso (la proprietà di non manifestare comportamenti che possano contribuire a causare danni ai pazienti). Ricordiamo che le due caratteristiche sono diverse e richiedono modi diversi per dare una ragionevole garanzia che il prodotto le possieda. Un prodotto software potrebbe essere molto affidabile, manifestando un numero molto basso di malfunzionamenti durante un lungo periodo d'esercizio, ma potrebbe causare gravi danni al paziente per quei rari malfunzionamenti. Ricordiamo anche che queste due caratteristiche non esauriscono l'insieme delle possibili "qualità" di un prodotto software. Non consideriamo a esempio l'usabilità e cioè la facilità d'uso del software.

Si può dare una ragionevole garanzia sull'affidabilità del prodotto, progettando e realizzando un adeguato insieme di casi di test. Considereremo casi di test di tipo "funzionale" e cioè prove di funzionamento per le quali la singola funzione (non l'intero programma che ha effetti sistemici che vanno considerati per se stessi) è una "scatola nera" che riceve dati di ingresso e comandi e produce risultati, senza che chi esegue il test conosca la struttura interna del software. Questo modo di operare è adeguato dal punto di vista di un utilizzatore del software, e parte dal presupposto che lo sviluppatore abbia già esaurito tutte le altre modalità di prova che considerano invece la struttura interna dei programmi.

Tre aspetti su cui fare le verifiche

Lo sviluppo di un piano di prove richiede la definizione di una strategia adeguata. Il software deve essere verificato da più punti di vista diversi che devono essere testati separatamente. Identifichiamo almeno i seguenti tre punti vista:

- l'insieme delle funzioni elementari, ognuna delle quali può essere eseguita da un utilizzatore. In questi sistemi ogni funzione è costituita da una o più maschere che permettono di interagire con una base di dati;
- l'insieme dei processi utente. Ogni processo (a esempio di prescrizione, preparazione e somministrazione di un ciclo di terapia protocollata in un sistema software che gestisce la prescrizione e somministrazione dei farmaci) è costituito da un flusso di attivazioni di più funzioni elementari da uno o più utenti (medico, farmacista e infermiere in questo caso);
- l'insieme dei vincoli che sono imposti allo svolgersi dei processi (a esempio una terapia "protocollata" può essere in stati diversi: prescritta, in corso, sospesa, terminata, e il passaggio da uno all'altro è soggetto a regole aziendali e operative).

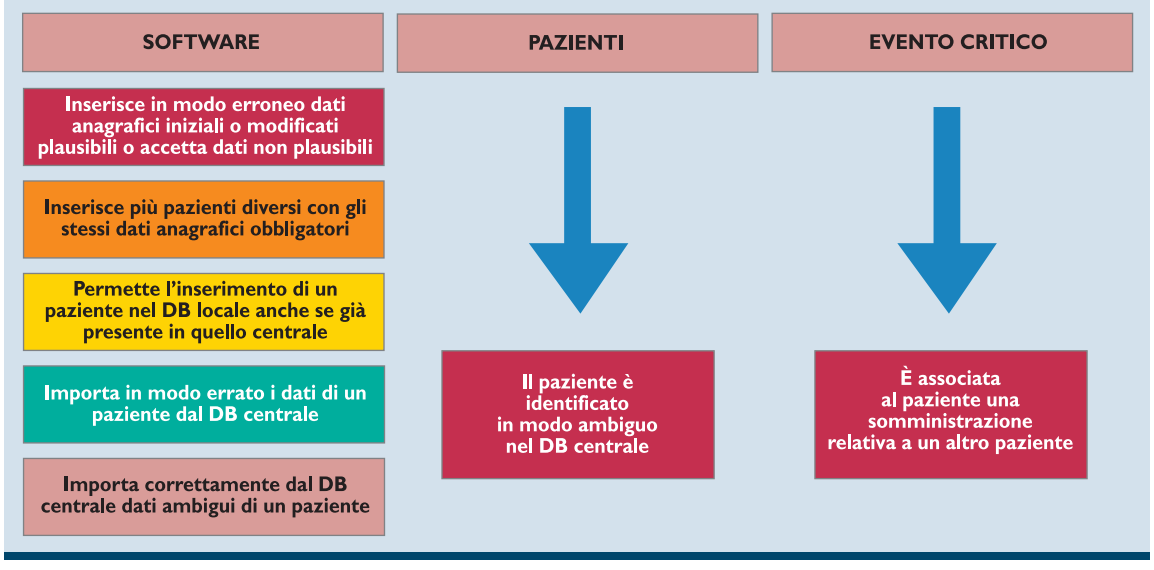
La verifica di aspetti diversi attraverso un piano di test è importante poiché ogni gruppo di test legato a un aspetto, può rilevare malfunzionamenti generati da diverse cause. A esempio, la verifica di ogni singola funzione può evidenziare problemi dovuti a un carente controllo dei dati di ingresso attraverso le maschere, mentre la verifica dei processi può rilevare problemi di interazione delle funzioni attraverso i dati dalla base dati o problemi dovuti a carenze di specifica.

In particolare sarà opportuno modellare i processi utente e gli insiemi di vincoli, con strumenti linguistici più rigorosi del linguaggio naturale, perché sia possibile applicare tecniche sistematiche, note da letteratura, per generare i casi di test.

L'elenco delle funzioni (con le associate specifiche), i modelli dei processi e i modelli degli insiemi di vincoli, sono la base per applicare le tecniche più adeguate allo stato dell'arte per produrre i casi di prova. L'attività di test fornirà un rapporto finale che include la descrizione della strategia e delle tecniche adottate, l'elenco dei casi di prova, l'esito di ogni caso e la documentazione che certifica l'esito.

È noto che non è possibile per un sistema software complesso, dimostrare la correttezza e cioè l'aderenza alle sue specifiche. È invece possibile produrre un rapporto di test che porti a una "ragionevole fiducia" nell'utilizzo, basato su un approccio robusto, ben fondato scientificamente e difendibile allo stato dell'arte davanti a una commissione di esperti. Egualmente importante è la valutazione di un software clinico per quanto riguarda la sua "sicurezza d'uso" (o, se vogliamo utilizzare il termine anglosassone, "safety", da non confondere con la "sicurezza" nel senso di privatezza, a esempio dei dati). Nella classe dei sistemi informativi utilizzati per applicazioni cliniche, un ruolo importante per la sicurezza d'uso è svolto dai dati. È infatti possibile che una condizione rischiosa possa essere causata non solo da un malfunzionamento del programma (un programma calcola in modo erroneo un dosaggio) ma anche da una configurazione errata dei dati (un programma copia correttamente da un'altra base dati nella

Esempio di tappe dell'analisi del rischio



servono certificazioni adatte alle caratteristiche

software sicuro

possibilità di ridurre gli eventi critici

Ospedali Riuniti di Bergamo: situazione a gennaio 2008

- **Dipartimento onco-ematologico:** 24 medici, 70 infermieri (oncologia medica, ematologia, Dh onco-ematologico)
- **Ortopedia e Traumatologia:** 20 medici, 50 infermieri
- **Dipartimento Chirurgico:** 50 chirurghi/anestesisti, 72 infermieri (chirurgia I e III, maxillo-facciale, plastica, senologica, toracica, anestesia I)
- **Dermatologia:** 6 medici, 5 inferm.ri
- **Pneumologia:** 15 medici, 18 infer.
- **Neurologia (degenza e Dh):** 13 medici, 37 infermieri
- **Pediatria:** 14 medici, 41 infermieri
- **Cardiochirurgia:** 13 medici, 37 infermieri
- **Ginecologia:** 13 medici, 38 infermieri
- **Ostetricia e sala parto:** 29 medici, 86 infermieri e ostetriche
- **Anestesia II:** 15 anestesisti (So cardiochirurgia, ostetricia/ginecologia, ortopedia)
- **Farmacia:** 5 farmacisti, 3 borsisti, 10 infermieri (laboratorio Umaca, laboratorio galenica, farmacoeconomia e logistica)
- **Sistemi informativi:** 2 ingegneri, 1 responsabile formaz./avviamenti
- **Pazienti distinti seguiti in FarmaSafe@:** più di 8.000 da maggio 2006

so è, per sua natura, uno strumento collaborativo che si propone di ricordare, ordinare, sistematizzare, semplificare, tenere traccia di tutte le azioni generate dalla cooperazione tra esseri umani, finalizzata a un obiettivo complesso, come può essere assicurare la cura ai degenti di un reparto ospedaliero. Bisogna pertanto prendere atto che questa tipologia di "oggetti" basa la propria efficacia non già sulla "chiusura", ma sull'apertura e adattabilità al mutevole agire dell'essere umano all'interno di una organizzazione.

Per proseguire nell'analisi, è necessario a questo punto definire con una certa precisione, dal punto di vista funzionale e dal punto di vista tecnologico, la categoria di oggetti dei quali stiamo trattando, e solo successivamente portare il dibattito sulle modalità di "certificazione".

Possono rientrare con vari livelli di appropriatezza nella categoria dei software di rilievo clinico, i sistemi di automazione di processi diagnostici (laboratorio-radiologia); di refertazione assistita; i software di gestione di processi terapeutici (prescrizione e somministrazione di farmaci e di emocomponenti); di gestione di protocolli di cura. Dal punto di vista tecnologico possono valere le seguenti caratteristiche: l'architettura software è costituita da una base di dati centrale e da una collezione di funzioni che operano sulla stessa; le funzioni non sono soltanto utilizzate per memorizzare dati ed eseguire interrogazioni, ma anche per processi aziendali; i processi sono vincolati da regole aziendali che tipicamente riguardano possibili evoluzioni dello "stato" di entità descritte nella base dati; specifici dati scorretti o specifici malfunzionamenti del software possono causare problemi di "sicurezza d'uso" (causare danni alla salute dei pazienti).

Per condivisa ammissione, tale categoria di prodotti software non è "certificabile" attraverso procedure di collaudo. Cosa è necessario fare pertanto, per garantirne l'affidabilità e, al contempo, la sicurezza d'uso? In primo luogo, va affrontato, con estrema cautela, il problema della "destinazione d'uso". Che utilità pratica può avere, infatti, dichiarare "dispositivo medico" e porre di conseguenza ferrei limiti al suo utilizzo e alla sua evoluzione, un prodotto che ha nella necessità di adattamento costante uno dei suoi principali requisiti funzionali? Non parliamo infatti di sistemi chiusi ma di sistemi "aperti", cioè modificabili in qualsiasi momento, e perciò soggetti a possibili condizioni di utilizzo non definibili e completamente prevedibili a priori. Bisogna pertanto passare a considerare l'ipotesi di una diversa, più adeguata, modalità di "certificazione" applicabile a questo genere di sistemi. Il modello metodologico che proponiamo è elaborato a partire da esperienze concrete maturate presso gli Ospedali riuniti di Bergamo.

pagine a cura di
PierMauro Sala
Ospedali Riuniti di Bergamo - Direttivo Aisis
Antonio Fumagalli
Ospedali Riuniti di Bergamo
Paolo Salvaneschi
Salvaneschi&Partners e Università di Bergamo

propria base dati, dati anagrafici che possono identificare erroneamente un paziente).

La sicurezza va verificata anche durante il processo di sviluppo del software, ma secondo il punto di vista dell'utente finale e quindi le verifiche che si concentrano sulle possibili interazioni tra le funzionalità disponibili. I criteri per la valutazione di sicurezza d'uso sono basati sull'identificazione di "eventi critici" pericolosi per la salute del paziente. Un esempio di evento critico può essere: «Viene associata al paziente una somministrazione relativa a un altro paziente».

Il metodo applica un'analisi di rischio al caso di un prodotto software che ha come componente una base di dati ed è composto dai seguenti passi:

- sono classificati gli eventi critici e identificati gli insiemi di dati (definiti "dati critici" come i dati anagrafici del paziente) nella base dati dell'applicazione che possono costituire, se alimentati erroneamente, condizioni che contribuiscono a un evento critico;
- per ogni condizione così identificata è modellato il grafo dei possibili eventi causati da funzioni software che possono generare la condizione;
- in generale esiste un numero limitato di funzioni software coinvolte. Per ognuna di esse sono considerati i test realizzati per verificare l'affidabilità ed eventuali altri test specifici al fine di produrre evidenza che sia possibile attivare gli eventi modellati.

Le prove effettuate non arrivano a dimostrare l'impossibilità di raggiungere l'evento critico, ma sono in grado di dimostrare la possibilità che dei malfunzionamenti identificati nel prodotto software o anche dei funzionamenti corretti ma pericolosi (a esempio l'input poco controllato di dati critici) contribuiscano a generare l'evento critico.

I risultati dell'analisi permettono di fornire suggerimenti per la modifica del software e la riduzione del rischio. Si ribadisce infine che la sicurezza d'uso è una proprietà di sistema.

L'evento critico dipenderà da un insieme di fattori che, in generale coinvolgono il software ma anche macchinari, persone e organizzazione.

Anche l'analisi di sicurezza d'uso rilascia un rapporto finale che descrive metodi e risultati e fornisce ragionevole e difendibile evidenza a supporto dell'utilizzo sicuro del prodotto.

Conclusione. Il processo di "certificazione", o di reale contenimento del rischio clinico, per questi prodotti, deve essere continuo e coinvolgere tecnologia, comportamenti personali e organizzazione.

Stiamo infatti parlando della necessità di indagare una proprietà concreta ed emergente dei sistemi, che definiamo "safety", che si realizza solo con l'apporto efficace e integrato di tutti gli attori: in primo luogo le persone. Poi hardware, software, dati, conoscenza, procedure organizzative e - in certi casi - anche "dispositivi medici".