Medicina Legale

Cosa pensare della documentazione informatizzata?

G. Martini
L. Perugia

La responsabilità medica in sede civilistica riguarda l'inadempienza nell'obbligazione di mezzi e di comportamenti e non di risultati; analogamente in sede penale è richiesto che il medico si attenga a regole doverose di condotta professionale (Cass. Pen. Sez. IV 30.04.1981 n. 4023 e Cass. Pen. 12.09.1970 n. 1386).
Appare quindi evidente la assoluta necessità che chiunque, anche non medico, esamini le caratteristiche di un comportamento debba necessariamente interpretarle in rapporto alla documentazione clinica del caso.
Di qui la determinante importanza della cartella clinica considerata "atto pubblico" (art. 2699 c.c.), provvisto di "efficacia probatoria" (art. 2700 c.c.).
Il documento clinico è "fide facente" ove risponda alle seguenti caratteristiche:
rappresentatività: la cartella deve rappresentare in maniera completa una raccolta di documentazione clinica in tutto il percorso assistenziale;
coevità: "il fatto clinico registrato dalla cartella deve essere annotato in modo coevo al suo verificarsi" (Cass. Pen. Sez. V 11.11.1983 n. 476); ne deriva la constatazione che ogni annotazione, anche singolarmente considerata, è provvista di un autonomo valore documentale definitivo;
certezza: "le modifiche e le aggiunte integrano un falso punibile, anche se il soggetto abbia agito per ristabilire la verità, perché violano le garanzie di certezza accordate agli atti pubblici" (Cass. Pen. Sez. V 23.03.1987);
definitività: compilata e sottoscritta la cartella acquista un carattere di assoluta definitività per cui "ogni successiva alterazione del suo contenuto costituisce il reato di falso materiale in atto pubblico" (Cass. Pen. Sez. V 03.05.1990);
coerenza: validi elementi di giudizio in merito al comportamento tenuto dai sanitari possono derivare dalla concordanza o dalla discordanza, sul piano della logica clinica, delle diverse annotazioni riportate.
Gli estensori della cartella clinica devono essere quindi consapevoli che la sua stesura rappresenta un obbligo di legge, una necessaria fonte informativa ed anche la garanzia di un corretto comportamento che il medico abbia, non solo tenuto, ma anche documentato in quello che può essere considerato un elemento probatorio in suo favore.
Attualmente necessità organizzative ed opportunità tecnologiche convergono nel richiedere l'informatizzazione della cartella clinica e, a questo punto, riteniamo di doverci porre alcuni interrogativi le cui risposte siano in grado di tutelare, anche in futuro, la documentabilità del comportamento che avremo tenuto nel singolo caso clinico.
Le perplessità delle quali in questa sede chiediamo un chiarimento alla Magistratura ed alle Società di informatica discendono dalle devianze che una cartella informatizzata può presentare nei confronti di quelle caratteristiche probatorie che abbiamo precedentemente descritto come ritenute cogenti dalla Suprema Corte.
Riflettiamo: una cartella clinica informatizzata può non essere coeva al verificarsi degli eventi clinici perché aggiunte od eliminazioni possono agevolmente essere effettuate in un periodo di tempo successivo; può non essere definitiva perché successivamente modificabile, anche se di una modificazione si possono rilevare tracce a distanza di tempo.
Il fatto di poter inquinare i criteri di coevità e di definitività può rendere, quindi, inapplicabili quelle garanzie di certezza che abbiamo visto essere fondamentali ai fini della rilevanza probatoria del documento.
La nostra perplessità poi si accentua ove si consideri la teorica permeabilità di un documento informatizzato e difficoltà tecniche nel rilevare dati in due sedi ospedaliere che siano provviste di network completamente differenti.
E' infatti in corso, proprio mentre esprimiamo queste perplessità, una competizione fra diversi produttori di

software, potenzialmente del tutto diversi fra loro, per assicurarsi il contratto con Sedi Ospedaliere nella fornitura dei mezzi informatici di documentazione medica.
Riteniamo quindi utile inserire, a questo punto delle nostre riflessioni, lo stato dell'arte relativo a: *La Cartella Clinica Informatizzata, Sicurezza e Validità Legale*.

L'archiviazione dei dati sanitari è stata, negli ultimi anni, una delle maggiori fonti di applicazione dell'informatica al fine di ottenere numerosi vantaggi sia in termini di tempo che di facilità di ricerca ed elaborazione dei dati, tipica dei "data-bases".
Questi, come tutti i sistemi informativi, dovrebbero rispondere ai seguenti requisiti: fornire l'informazione che serve, dove serve, nel modo adeguato, sempre e solo quando serve, ed esclusivamente a chi è deputato a farne uso.
La cartella clinica costituisce un esempio complesso di sistema informativo che tende, sempre più, ad essere gestita a mezzo di strumenti informatici da parte degli operatori che, come per la formulazione cartacea, non sono solo medici o specialisti ma anche infermieri, assistenti sociali, personale amministrativo e giudiziario.
I dati contenuti all'interno della cartella clinica sono di grande importanza non solo nell'attività relativa all'evento corrente, ma anche a distanza in occasione di revisioni dei dati.
Gli operatori sanitari possono essere pertanto interessati, in tempi diversi e a vario titolo, ad utilizzare i dati clinici quotidianamente accumulati.
Anche altri operatori dell'ambiente sanitario, e non, possono essere istituzionalmente tenuti a revisionare alcuni dati.
La delicatezza dei dati clinici, quindi, impone controlli sugli accessi, per garantire che essi siano gestiti solo da personale esperto ed avente titolo a dedicarvisi: devono essere evitati da una parte l'intervento di operatori non addestrati ad immettere informazioni (che compromettano la qualità dei dati), dall'altra l'intrusione di operatori non accreditati, che accedano al sistema per scopi estranei alle esigenze istituzionali.
Un buon database (come la cartella clinica) deve pertanto essere dotato di un ragionevole livello di sicurezza ed organicità nel controllo degli accessi.
Il meccanismo comunemente utilizzato è quello della Password Alfanumerica ossia, di regolamentare l'accesso richiedendo, in apertura della sessione di lavoro, la dichiarazione del nome e di un codice di riconoscimento da parte dell'operatore.
Nome espresso esplicitamente e codice (password) espresso in modo mascherato vengono confrontati con il contenuto di una tabella predefinita e solo chi risulta accreditato può essere autorizzato ad accedere al sistema.
La dichiarazione della password serve al computer per riconoscere la mano dell'operatore e dargli accesso al sistema; inoltre questa forma di firma elettronica può essere utilizzata per marcare i dati immessi, consentendo di attribuire la responsabilità della sessione di lavoro.
Teoricamente ogni accesso potrebbe essere registrato e per ogni dato potrebbe essere segnalato il momento dell'immissione o modifica.
In realtà pensando al gran numero di dati usualmente contenuti nel database, è sostanzialmente improponibile attuare una registrazione analitica così completa degli accessi.
Viene di solito ritenuto sufficiente registrare per ogni record il nome e la data di accesso dell'ultima revisione: ad ogni revisore si attribuisce la responsabilità di accreditare non solo le correzioni svolte, ma anche la verifica dei contenuti precedentemente immessi nella tabella (o almeno la verifica di congruità e verosimiglianza con quanto immesso nella corrente sessione di lavoro).
La dichiarazione della password consente di identificare la tipologia dell'operatore. Per ogni operatore può essere imposta una strategia personalizzata di accesso ai dati, definendo l'ambito di visibilità ed i gruppi di funzioni accessibili.
Nella pratica il sistema della password è meno sicuro di quanto dovrebbe; non è infrequente che un operatore abbandoni il computer nel mezzo di una sessione di lavoro, magari chiamato con urgenza ad altri compiti, lasciando in fase di visualizzazione il set di dati in corso di analisi.
In molte situazioni esiste una modalità di lavoro di gruppo, per cui più operatori accedono a turno ad una stessa postazione per immettere dati nell'archivio; di fatto è relativamente frequente che una sessione iniziata da un operatore venga proseguita o continuata da altri del gruppo.
Una delle precauzioni possibili consiste nel forzare l'utente a dichiarare le proprie generalità informatiche in particolari condizioni: si può imporre che venga richiesta ripetutamente la password in base alla circostanza o alla cronologia degli eventi. Può essere per esempio richiesta la password ogni volta che viene aperta una nuova scheda, per evitare che un'intera seduta di lavoro, registrata a più mani, venga accreditata ad un identico operatore. Oppure può essere abbinato un meccanismo di richiesta di password a tempo: anche all'interno della

stessa procedura, dopo un tempo di inattività ritenuto significativo, l'operatore può essere automaticamente richiesto, alla ripresa del lavoro, di dichiarare le proprie generalità, per garantire che sia sempre adeguatamente autorizzato all'accesso.
Tali accorgimenti costituiscono un livello di protezione ragionevole per verificare gli accessi senza appesantire troppo il lavoro degli operatori.
Non sono tuttavia una garanzia assoluta di protezione da accessi indesiderati, perché non sempre il sistema delle password riesce ad essere gestito con assoluta riservatezza (per situazioni contingenti in cui risulta necessario dichiararla apertamente, oppure per disattenzione al problema da parte degli operatori).
La politica della periodica sostituzione della password, pur essendo consigliata, risulta di fatto spesso disattesa, per motivi di inerzia sia del sistemista sia degli operatori. Questi ultimi, in particolare, sono resistenti per il fatto che spesso devono gestire numerose chiavi di accesso personali in differenti sistemi e la frequente sostituzione può diventare fonte di scorrettezze procedurali.
In ogni caso il computer non può distinguere se dietro una password accreditata si nasconda un operatore effettivamente idoneo all'ingresso oppure un intruso, che cerchi di forzarne l'uso.
Sono stati introdotti, negli ultimi anni, sistemi di riconoscimento degli operatori più sicuri della semplice password, per ora utilizzati,solo sporadicamente, in campo sanitario, anche se nel prossimo futuro ne è prevedibile la diffusione.
Un livello superiore alla semplice password consiste nel prevedere che i dati di qualifica personale vengano dichiarati non solo da tastiera, ma mediante un supporto magnetico personale (card), di cui sia prevista una sola copia assegnata ad ogni utente ossia mediante Carta Magnetica.
Un documento elettronico del formato e del tipo della carta di credito ha un costo modesto e può essere caricato di numerosi dati di riconoscimento, che aumentano la sicurezza del sistema: l'operatore, pur incline a non praticare una politica di riservatezza della propria password, dovrà porre certamente più attenzione al problema se l'accesso al sistema può avvenire solo mediante dichiarazione contemporanea di alcuni dati da tastiera e di altri tramite immissione della propria scheda personale in un apposito lettore.
Questo livello di sicurezza impone costi e organizzazione più elevati: ogni operatore deve possedere una carta di riconoscimento; ogni postazione deve possedere un lettore di carte; deve essere garantito un sistema di generazione e sostituzione delle carte in caso di smarrimento; soprattutto deve essere predisposta una politica attenta nella scelta degli standard, in un campo, quello delle carte magnetiche, ancora non assestato, nel quale gli standard di formato e di prestazioni sono in continua evoluzione.
Per situazioni particolari si stanno iniziando ad utilizzare metodi di controllo ancora più sofisticati ossia Tecniche Biometriche.
La veridicità della dichiarazione elettronica può infatti venire sottoposta a validazione mediante analisi di caratteristiche fisiche personali dell'operatore, quali il timbro della voce o l'immagine dell'iride.
È relativamente facile fornire un computer di un sistema di riconoscimento vocale che permetta di controllare la corrispondenza tra i dati personali dichiarati ed il relativo timbro di voce, preventivamente classificato e archiviato.
Ovviamente le esigenze aumentano in termini di hardware e di software: i computer devono essere equipaggiati con sistemi multimediali per l'acquisizione della voce dell'operatore e di software adeguato.
Possono poi verificarsi problemi non banali in caso, ad esempio, di affezioni respiratorie che alterino il timbro di voce dell'operatore.
In sintesi, esistono diversi modi di verificare gli accessi al sistema ed è possibile associarli fino ad arrivare ad un livello analitico di verifica molto complesso e sicuro. La definizione della politica di controllo degli accessi deve essere impostata sulla base del tipo di dati (grado di riservatezza), dell'architettura del sistema (disposizione delle postazioni), dell'omogeneità e motivazione degli operatori previsti, e del rischio effettivo di subire intrusioni incongrue. Occorre infatti tarare il grado di controllo su un livello di ragionevole compromesso tra le esigenze di riservatezza e l'inopportunità di ostacolare frequentemente l'operato degli utenti con il noioso meccanismo di dichiarazione delle proprie generalità informatiche.
In fine per essere efficaci, i sistemi informatici devono prevedere un sofisticato grado di condivisione in rete delle informazioni.
Il principio di condivisione suggerisce che ogni dato debba essere immesso solo una volta nel sistema e, dopo essere stato attentamente validato, venga messo automaticamente a disposizione di qualunque operatore ne abbia necessità e autorizzazione.
La Condivisione Dei Dati riguarda soprattutto gli operatori di ogni singolo gruppo, ma si allarga in alcune circostanze a tutti coloro che svolgono attività adesso collaterali.

Spesso è interesse reciproco tra differenti gruppi di lavoro, che traggono vantaggio dalla condivisione di parte dei relativi archivi. Esempio classico è quello delle interazioni tra una divisione clinica e un servizio diagnostico: i clinici hanno senza dubbio beneficio dalla visibilità dei dati prodotti dal servizio (laboratorio analisi, radiologia), il quale d'altra parte si può avvantaggiare ricevendo ad esempio informazioni cliniche o amministrative direttamente dai reparti, semplificando l'assolvimento dei propri compiti istituzionali.
A questo scopo si devono verificare due condizioni fondamentali: l'esistenza di una connessione fisica tra i sistemi informativi dei due gruppi (rete locale) e la strutturazione della connessione funzionale tra i relativi software, per rendere la procedura trasparente (cioè semplice ed immediata) ai rispettivi operatori.
Occorre definire la politica degli accessi ai due sistemi, nel rispetto della necessità di garantirne sicurezza e riservatezza adeguate.
(A cura di D. Palmieri e L. Ottaviano)

I clinici ed i medici legali più versati nelle tecniche digitali ci informano che la cartella clinica informatizzata:

1) può essere modificata in tempi successivi agli eventi; di tale penetrazione rimane una traccia, senza che essa possa essere attribuita ad alcuno;
2) la penetrabilità del documento può configurare violazione del segreto professionale (art. 622 c.p.);
3) la cronologia della documentazione può essere compromessa dalle modifiche, e rende quindi il documento aperto ad un numero illimitato di successive manipolazioni.

Le considerazioni che abbiamo espresso sono certamente improntate ad una perplessità che, d'altra parte, appare giustificata della costante espansione di quella epidemiologia giudiziaria che sembra connotare, in maniera sempre più incisiva, l'analisi, troppe volte manichea, del comportamento con il quale i medici possano dimostrare di aver affrontato le infinite incognite di un divenire patogeno incerto, perché biologico.
La prova documentale rischia, quindi, di veder diluita in infinite incertezze la sua intrinseca capacità probatoria di un determinato comportamento.
Ma è anche l'unico elemento che il medico corretto possa invocare come giustificazione di un difetto di risultato del quale può essere responsabile un concorso di condizioni antecedenti e di concause sopravvenute.
Abbiamo in conclusione il timore, speriamo infondato, che l'incertezza probatoria del comportamento, quale può essere riscontrato in una cartella informatizzata, possa indirizzare la Magistratura inquirente a privilegiare la valutazione del risultato raggiunto, spostando, così, radicalmente, il rapporto fra la valutazione del comportamento e quella del risultato che attualmente richiede prove certe (Sez. Unite Corte Cass. sent. n. 30328, 11.09.2002).
La domanda che crediamo di dover rivolgere a chi ci ha fin qui seguito è apparentemente semplice:
la documentazione informatizzata è in grado di fornire prove certe?
Riteniamo, a livello del tutto personale, che la risposta possa essere negativa e positiva quando si considerino le differenti ragioni che possono richiedere la consultazione di tale documento:
a finalità giudiziarie, la cartella clinica deve essere olografa, cartacea e firmata da uno o più responsabili nei punti salienti della sua stesura (ad esempio descrizione dell'intervento, consulenze di altre specialità, accertamenti di laboratorio, ecc.); quanto precede è del tutto analogo alle procedure eseguite nei verbali di udienza dei Tribunali;
a finalità conoscitiva dei dati clinici, ad esempio nella prosecuzione di un trattamento presso altre sedi, ed a scopo di ricerca epidemiologica; in tali casi la trasmissione di dati informatizzati può presentare indubbi vantaggi in termini di tempo e di esaustività di informazione; ma anche in questi casi, la divulgazione deve essere resa lecita da un consapevole consenso del malato in merito alla possibilità, anche teorica, che quanto lo riguarda venga sottratto alla riservatezza che deve connotare ogni attività clinica.

BIBLIOGRAFIA

Ciallella C, Colesanti C. *Il segreto professionale nell'archiviazione informatica di dati sanitari* Riv It Med Leg 1991.

Ravizza P, Pasini E. *Informatizzazione della cartella clinica: aspetti medico-legali, privacy, sicurezza e validità*. Ital Heart J Suppl 2001;2:268-86.

Nonis G, Braga M, Guzzanti E. *Cartella clinica e qualità dell'assistenza: passato, presente e futuro*. Roma: Il Pensiero Scientifico Editore, 1998.

Millman A, Lee N, Brooke A. *Computers in general practice I-II-III. BMJ 1995 Smith AP. Design a clinical information system*. BMJ 1992;305:415-7.

Wyatt JC. *Clinical data systems. Part 1: data and medical records*. Lancet 1994;344:1543-7.

Wyatt JC, Wright P. *Design should help use of patients' data*. Lancet 1998;352:1375-8.

Wyatt JC. *Clinical data systems. Part 2: components and techniques*. Lancet 1994;344:1609-14.