Banche dati, registri e schedari in ambito sanitario: aspetti legali

G. Casiraghi[a], M. Pradella[b]

[a]*Gruppo di Studio Risk Management SIMeL*
[b]*Gruppo di Studio Informatica SIMeL*

Riassunto. La documentazione sanitaria riveste una notevole importanza come prova dell'attività sanitaria e ciò nonostante è uno degli aspetti meno conosciuti del rapporto tra le strutture sanitarie e gli *stakeolders* della sanità. Viene trattata la recente legislazione in ambito sanitario, con particolare riguardo alla recente legge 196/2003, meglio conosciuta come "Codice della Privacy" con gli adempimenti legislativi e organizzativi connessi alla gestione delle banche dati sanitarie informatizzate e non, con particolare riferimento al servizio di Laboratorio Analisi. Si forniscono soluzioni per gli adempimenti legislativi correlati alla gestione degli archivi sanitari, allo scopo di consentire un più facile adeguamento alle leggi.

Abstract. Health documentation has a significant importance as a proof of health activity, though it is one of the less known aspects of the relation between health structures and health stakeholders. The recent laws within health environment are treated here, in particular Law 196/2003, better known as the "Privacy Code", together with the legislative and organization implementations in relation to health data banks, both computerized and not, with a specific reference to the Clinical Laboratory service. Solutions are proposed for the legislative implementations linked to the management of health files for the purpose to make adjustment to the laws easier.

Introduzione

La tenuta della documentazione sanitaria rappresenta uno degli aspetti più misconosciuti dell'attività di assistenza che viene fornita ogni giorno, in Italia e all'estero. Pochi, infatti, pensano alla gestione degli archivi come ad una "funzione strategica" del servizio o dell'attività svolta a favore dei cittadini. Pochissimi poi ne sondano gli aspetti organizzativi, specie degli obblighi di conservazione nel tempo. Al contrario, gli aspetti gestionali e legali presuppongono una "ingegnerizzazione del problema" con soluzioni operative anche estremamente complesse. Rientriamo comunque nella vasta tipologia della comunicazione medico – paziente e, pur dovendo considerare l'atipicità di una situazione comunicativa (in cui possono essere assenti il primo, il secondo od entrambi), cercheremo di sintetizzare alcuni punti essenziali del problema.
Per prima cosa è importante definire la visione prospettica del problema, specie per la variabile *tempo* e per quella *tipologia dei dati sanitari*. Vedremo anche altri due aspetti relativi al *chi* deve conservare i dati sanitari e *con quali mezzi*. Variabile temporale: differente è conservare della documentazione sanitaria per un'anno, per tre anni, per dieci anni o "per sempre", specie in quest'ultima eccezione (quanto è, in termine di anni, "per sempre"? Per cento anni, per mille anni?). La tipologia dei dati sanitari è decisamente non uniforme: differente è che si parli di cartella clinica (e delle parti che concorrono alla sua formazione), di esami strumentali, di visite, di terapie di registri (operatori, stupefacenti, ecc.). L'assistenza poi, specie nelle strutture sanitarie come ospedali e poliambulatori non è fornita da un solo sanitario, ma da un'equipe con numerosità e ruoli differenti: chi tra questi deve assicurare la conservazione del dato sanitario? Chi lo deve fornire al paziente? Ammesso di aver risolto più o meno brillantemente tutti i precedenti quesiti rimane poi l'aspetto tecnico, il come conservare i dati sanitari, come si dice oggi, su supporto cartaceo od informatico?
Ma se non si è in grado di dire che cosa vogliamo che accada non abbiamo identificato i problemi, stiamo solo lamentandoci. Un problema esiste solo se c'è differenza tra ciò che sta accadendo e ciò che vorremmo accadesse. Il "ciò che sta accadendo" è la vita di tutti i giorni nelle nostre rispettive realtà, il "ciò che vorrem-

Corrispondenza a: Dott. Giovanni Casiraghi. E-mail: giovanni.casiraghi@asl.como.it.

mo accadesse" è che le leggi fossero le regole a cui attenerci. Ma la maggior parte di noi non ha familiarità con le leggi dello Stato e con quello che motiva tali leggi.
Uno sforzo per chiarire il problema è "di che cosa abbiamo bisogno" per evitare il sovradosaggio di dati sanitari. È nozione comune a tutti che in campo sanitario disponiamo di una quantità di dati che rischia di portare ad una crisi di sovrasaturazione, specie per quanto riguarda diagnostica e terapia. Non tutto va archiviato e sicuramente non per lo stesso tempo e nello stesso modo. Abbiamo bisogno sicuramente di due tipi d'archivio, uno d'uso ed uno storico. Il primo viene gestito direttamente da chi ne ha la responsabilità legale e deve consentire una rapida restituzione dei dati richiesti. Il secondo non ha l'urgenza della restituzione dei dati, può essere gestito "in differita".
La gestione dei dati sanitari ha una sua propria "evoluzione logica": da sempre il primo aspetto ad essere affrontato ed informatizzato è quello della gestione amministrativa, risolta la quale viene affrontata la gestione dei Servizi che formalizza chi fa cosa con quali risorse. Realizzate queste prime due fasi ci si rivolge "all'esterno" per realizzare una integrazione tra le strutture sanitarie (terza fase) propedeutica alle funzioni epidemiologiche e di controllo caratteristiche della quarta ed ultima fase. Tutte queste fasi sono legate ad un continuo alternarsi dinamico di input *top down* e *bottom up* che ne condizionano la crescita. In tale ottica, la legislazione ci fornisce indicazioni sia di pianificazione sia di comportamento etico in tutte le fasi sopra descritte chiaramente "top down".
La componente sanitaria non può che far riferimento ad un modello semantico per risolvere il problema, essendo quello sanitario principalmente un sistema decisionale: altrimenti i dati da una parte e gli obblighi legislativi e gestionali dall'altro ci portano inevitabilmente a rimanere stritolati dal sistema.
Solo un modello semantico è infatti in grado di adattarsi a nuove regole mantenendosi costantemente aggiornato nel tempo al variare delle leggi e delle richieste. Sicuramente utile è la formalizzazione di tali concetti realizzata da Elmer R. Gabrieli quasi trent'anni orsono[1] e a tutt'oggi valida.
Veniamo agli aspetti legali: essi sono riferiti alla documentazione in generale (atti pubblici) ed a specifiche situazioni, come cartelle cliniche, registri, documenti particolari. La situazione è in alcuni insiemi sovrapponibile a quella riguardante il referto di laboratorio, avendo in comune le componenti generali riguardanti la descrizione della conservazione dei dati e la gestione di laboratorio sfociante nella normativa internazionale e in quella ISO in particolare[2].
Il corpo legislativo è estremamente vario e complesso e peraltro già oggetto di articoli specifici[3] anche per le modalità di finanziamento ad esse correlate che hanno imposto alla classe medica una serie di comportamenti che implicano un adeguamento culturale prima che professionale[4].

La legislazione recente

Preme comunque inquadrare la legislazione più recente, in larga parte disattesa, per fornire un aggiornamento attualizzato alla luce delle leggi più recenti.
Come primo riferimento legislativo riassumiamo i punti salienti del Decreto del Presidente della Repubblica 14 gennaio 1997 soprannominato "Accreditamento"[5] dal punto di vista del Laboratorio Analisi. Quest'ultimo risulta tenuto agli archivi degli esami effettuati (un anno) e dei controlli di qualità (tre anni). Non viene fatta menzione di che caratteristiche deve avere l' archivio, ma la legislazione nazionale precedente identifica comunque un obbligo differente per la conservazione della risposta ambulatoriale, inquadrandola come documentazione sanitaria, mentre per i pazienti ricoverati diventa allegato della cartella clinica.
Per i dati ambulatoriali la conservazione di un anno non è comunque in linea con la conservazione dei dati sanitari (l'obbligo legislativo considera dieci anni): un'accattivante interpretazione è che il laboratorio è tenuto alla conservazione dell'archivio "vivente" per un anno, mentre per il tempo rimanente si possono utilizzare diverse soluzioni, concordate con la direzione sanitaria, riguardanti l'archivio storico.
Tale soluzione può essere estesa anche agli "allegati della cartella clinica" che dopo il primo anno possono essere archiviati in altro Servizio sotto la diretta gestione della direzione sanitaria aziendale. La cartella clinica, da considerare atto pubblico[6], deve essere infatti conservata "per sempre[7] e gli allegati non meno di dieci anni e vanno a costituire una parte dell'archivio storico affidato alla Direzione Sanitaria. Bisogna considerare poi che gli esami comprovanti una diagnosi (specie se di quelle citate nella scheda di dimissione ospedaliera), diventano parte essenziale della cartella stessa, con valenza di "dato oggettivo" comprovante la diagnosi.
Questa è una significativa modifica legata ai cosiddetti DRG, probabilmente non sufficientemente conosciuta e compresa. Creato negli USA, il sistema dei DRG's (Diagnosis Related Groups) in varie delle sue versioni HCFA (Health Financing Administration release 10, 14, 19), è stato adottato dallo Stato italiano e dalle varie regioni, riunendo in circa 500 DRG classi omogenee di pazienti. Tale classificazione si basa su dati ottenibili alla dimissione del paziente quali le diagnosi, i tipi di interventi chirurgici e le procedure attuate, "filtrati" dallo stato di salute alla dimissione e da altri dati demografici. Tali dati dovrebbero teoricamente essere presenti nelle cartelle cliniche e basterebbe la corretta compilazione di una SDO (Scheda di Dimissione Ospedaliera) per poter classificare ogni paziente secondo un DRG appropriato. Nella SDO vengono utilizzati i codici ICD-9 CM (Clinical Modifications) per la diagnosi principale, le secondarie, per gli interventi e le procedure, codici basati su un sistema di codifica nosologica edito in Italia a cura dell'Istituto Centrale di Statistica (ISTAT,1984) col nome di "Classificazione delle malattie, traumatismi e cause di morte" che è a sua

volta il recepimento del Manual of the International Classification of Diseases basato sulle raccomandazioni della IX conferenza di revisione (ICD-9 Ginevra 1975) e pubblicato dall'Organizzazione Mondiale della Sanità.
Questa modifica è per certi aspetti rivoluzionaria: viene introdotto un lessico medico standardizzato[1], utilizzato su base mondiale, edito a livello nazionale italiano dal Poligrafico[8] con versioni regionali come la lombarda[9].

Il Codice della Privacy

Questo ci riporta alla gestione dei dati in ambito sanitario, dove dobbiamo inevitabilmente tener conto di tale novità, come pure della gestione degli archivi cartacei e non e delle problematiche legate alla firma elettronica. Infatti se l'atto di scegliere è fenomeno soggettivo e personale, nell'immagine ideale di ciò che vogliamo non possiamo esimerci dall'affrontare questi temi legali per realizzare un modello che comunque tenga conto di questi vincoli.
Che la legge 196/2003, meglio conosciuta come Codice della Privacy, sia una legge quadro di notevole spessore è evidente nel corpo legislativo (conta ben 186 articoli) e dal commento di recente realizzazione ad opera di 63 autori[10]. In particolare poi l'art. 94 fa riferimento a "Banche di dati, registri e schedari in ambito sanitario" riportando al primo comma *"1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso: …omiss… e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella Gazzetta Ufficiale n. 78 del 3 aprile 2001*". Questo articolo ci vincola tutti, ed in particolare per il trasfusionale, a nuove regole contenute nel Codice stesso[11].
Il recente Codice della Privacy sottolinea nuovamente i concetti di difesa perimetrale dei dati, di *Disaster Recovery*, di autenticazione e di autorizzazione estesa, specie in riferimento ai dati sensibili.
Che tale aspetto sia particolarmente gravoso per chi gestisce tali dati è stato di recente evidenziato dal rinvio dal 30 giugno al 31 dicembre a cui è stato sottoposto l'Art. 180 della 196/2003. L'Articolo recita al comma 2 "*Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura*." L'articolo prosegue con il comma 3: "*Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro un anno dall'entrata in vigore del codice*". C'è bisogno di una "interpretazione legale" articolata, basata anche su documentazione in parte già utilizzata dal Garante della Privacy nella precedente legge (675).
Illuminante è l'Art. 31 che al primo comma recita: "*1. i dati personali oggetto di trattamento sono custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta*". In sostanza è un articolo che presuppone un adeguamento continuo allo stato dell'arte informatica, un controllo dello stato degli archivi con almeno una copia dell'archivio stesso. Nel caso che la copia venga conservata in una sede fisicamente diversa dalla principale si verifica l'ottemperanza al concetto di *disaster recovery*. Così come la protezione dagli accessi non autorizzati apre la porta alla crittografia, assolutamente necessaria nel caso di accesso ad internet e codificata e diffusa in varie forme dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione)[12,13].
Veniamo ora agli specifici articoli che definiscono l'ambito riguardante le ***misure minime di sicurezza*** per Banche Dati ed Archivi.
L'Art. 33 "Misure minime" ribadisce "*1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali*". In sostanza vale quanto già accennato per l'Art.31.
L'Art. 34 "Trattamenti con strumenti elettronici" invece ci introduce alle regole per i data base (DB): "*1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g) tenuta di un aggiornato documento programmatico sulla sicurezza; h) ado-*

zione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari". Questo articolo, a ben vedere, ci obbliga a prendere in considerazione i vari aspetti della gestione degli archivi delle risposte che abbiamo fornito e ci sottolinea come devono essere realizzati i nostri progetti di informatizzazione dei laboratori per quanto riguarda la gestione degli archivi informatizzati. Viene da sottolineare in particolare il punto g), cioè il documento programmatico sulla sicurezza dei DB, che difficilmente fa parte del corredo di documentazione disponibile nei nostri laboratori. Sicuramente molto ancora c'è da fare. Se poi la difficoltà di gestione del DB ci spingesse a adottare il cartaceo in alternativa all'elettronico, è bene tener presente che anche questa soluzione è tenuta al rispetto dell'Art. 35 "Trattamenti senza l'ausilio di strumenti elettronici". Il primo comma definisce le regole: "*1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati*". Ci troviamo quindi nella necessità di affrontare tali problematiche.

Possibili Soluzioni

Una buona fonte è la *descrizione generale delle misure adottate per la sicurezza dei dati* (lett. D modello di notifica al Garante per la protezione dei dati personali ex 675/96 e delibera del garante 29 febb 2001, n.8) che suddivide il trattamento in automatizzato, non automatizzato e definendo le misure adottate graduate per classi di dati. Vengono anche suddivise le misure adottate in organizzative, fisiche e logiche.
Delle *organizzative* fanno parte: analisi dei rischi, prescrizioni di linee guida di sicurezza, altre istruzioni interne, assegnazione di incarichi, redazione di appositi mansionari, formazione professionale, classificazione dei dati, registrazione delle consultazioni, documentazione dei controlli periodici, verifiche periodiche su dati o trattamenti non consentiti o non corretti, distruzione controllata dei supporti, piano di *disaster recovery*, ecc.
Per le *misure fisiche* troviamo: vigilanza della sede, ingresso controllato nei locali ove ha luogo il trattamento, sistemi di allarme e/o di sorveglianza antintrusione, registrazione degli accessi, autenticazione degli accessi, custodia in classificatori o armadi non accessibili, custodia in armadi blindati e/o ignifughi, deposito in cassaforte, custodia dei supporti in contenitori sigillati, dispositivi antincendio, continuità dell'alimentazione elettrica, controllo sull'operato degli addetti alla manutenzione, verifica della leggibilità dei supporti, ecc.
Citate nelle *logiche* sono: identificazione dell'incaricato e/o dell'utente, autenticazione dell'incaricato e/o dell'utente, controllo degli accessi a dati e programmi, registrazione degli accessi, controlli aggiornati antivirus, sottoscrizione elettronica, cifratura dei dati memorizzati, cifratura dei dati trasmessi, annotazione della fonte dei dati, annotazione del responsabile dell'operazione, rilevazione di intercettazioni, monitoraggio continuo delle sessioni di lavoro, sospensione automatica delle sessioni di lavoro, verifiche periodiche su dati o trattamenti non consentiti o non corretti, verifiche automatizzate dei requisiti dei dati, controllo sull'operato degli addetti alla manutenzione, controllo dei supporti consegnati in manutenzione, ecc.
Ovviamente non vuol dire che tutte queste misure sono necessarie, ma sicuramente ci forniscono le coordinate di che cosa il Garante si aspetta come misure di protezione dei dati.
Abbiamo iniziato l'iter della nuova legge con l'Art. 180 ed ora lo riprendiamo per definire meglio il documento a data certa o Documento di Programmazione della Sicurezza (DPSS) a cui sono tenuti i responsabili di banche dati. La soluzione è stata proposta con la Direttiva del Presidente del Consiglio dei Ministri del 16 gennaio 2002 per la "Valutazione del livello di sicurezza delle banche dati"[14]. Di tale direttiva ci interessa in particolare l'allegato I, che ci consente di autovalutare lo stato dell'arte delle banche dati che ci riguardano e contemporaneamente, se lo datiamo e firmiamo, il DPSS di partenza. Il questionario è stato impostato al fine di consentire un processo operativo affidabile e rapido. A tale scopo sono state definite sei schede, una per ciascuna delle sei aree chiave della sicurezza: policy, ruoli e responsabilità, norme e procedure, amministrazione della sicurezza, analisi del rischio, formazione e sensibilizzazione. Ogni scheda comprende una lista di modalità operative, una guida alle domande che dovrebbero essere poste ed un insieme di possibili risposte (quattro) nell'ambito delle quali ci dovrebbe essere quella maggiormente coerente con la situazione riscontrata. Valutare la scheda comporta semplicemente selezionare una delle quattro possibili risposte predefinite su ciascuna delle sei schede. Perché farlo? Perché rientra nella sfera etica, e perché chi non predispone il DPSS e non adotta tutte le misure minime di sicurezza dal primo di gennaio rischia delle sanzioni[15].

Sanzioni

Amministrative: omessa o idonea informativa: € 3.000-18.000; omessa informativa in caso di trattamenti che se male effettuati mettono a rischio libertà

fondamentali: € 5.000-30.000; cessione di dati ad esercente non interessato alla salute del paziente: € 500-3.000; comunicazione dei dati da persona non titolata a conoscerli: € 500-3.000; omessa o incompleta notificazione: € 10.000-60.000; omessa informazione del Garante od omessa esibizione dei documenti richiesti dal Garante: € 4.000-24.000.
Penali: omissione di misure di sicurezza: reclusione 6-24 mesi; trattamento in presenza di rigetto dell'autorizzazione o di pendenza: reclusione 3-24 mesi; false dichiarazioni o false notificazioni al Garante reclusione: 6-36 mesi (ulteriore pena se c'è danno); trattamento di dati sensibili senza titolo al fine di recare profitti o recare danni ad altri: reclusione 6-24 mesi (ulteriore pena se c'è danno).

Firma elettronica, Crittografia e Carta Regionale dei Servizi

Per la firma elettronica una buona guida è fornita dal CNIPA[12,13], anche nel formato CD di e-learning, che riassume la normativa nazionale ed europea, costituita da oltre una decina di leggi e circolari ed in particolare dal Decreto legislativo 10/2002, che recepisce la legislazione europea e chiarisce i livelli di firma (firma elettronica, firma elettronica avanzata, firma elettronica avanzata prodotta con dispositivo di firma sicuro, firma digitale). Anche la crittografia è sufficientemente trattata nella documentazione del CNIPA dove vengono affrontati i concetti (chiave privata, chiave segreta, canale sicuro, repository locale, algoritmi simmetrici ed asimmetrici) legati alla problematica.
Parlando poi di soluzioni, un cenno sul progetto lombardo della Carta Regionale dei Servizi[16] è d'obbligo. Tale progetto è partito nel 2003 e dovrebbe essere completato entro il 2005. Basato su una card con microcip distribuito ai cittadini ed integrato da un sistema di rete a tre livelli, dominio centrale – provider – utenti sanitari, dovrebbe diventare il sistema di comunicazione regionale. Particolarmente interessante risulta il workflow di una prestazione di laboratorio, dove vengono identificati i vari attori coinvolti nella prestazione. Nel workflow è poi significativo che il depositario della risposta (refertazione) risulta essere il cittadino, dopo il passaggio dal medico di base prescrittore.

Conclusioni

Sicuramente siamo di fronte ad un forte fattore di cambiamento che si identifica con gli obblighi di legge nella gestione degli archivi e con le nuove regole comunitarie. Tali leggi, anche perché "europee", condizioneranno inevitabilmente il rapporto tra i gestori degli archivi sanitari e non e i cittadini. Diventerà inevitabile dedicare una "quota" del tempo lavorativo, specie per alcune figure professionali, agli obblighi gestionali introdotti dalle nuove leggi, in particolare per quelli legati alla 196/2003. Quest'ultima, oltre al cambio delle regole sulle banche dati ed archivi, modificherà sensibilmente il rapporto medico – paziente ed in definitiva le fasi pre- e post – analitica.

Bibliografia

1. Gabrieli ER. Interfaccia uomo-macchina. In Casiraghi E, Spaggiari P. Informatica Medica. Milano: Jackson Ed.;1987. p. 79.
2. ISO/PDTR 22869: Guidance on laboratory implementation of ISO 15189. Milano: UNI; 2004.
3. Casiraghi G. Linee Guida e Normativa. Riv Med Lab – JLM 2001; 2:61-5.
4. Benucci G, Bacci M, Pezzulli S, Carlini L, Suadoni F, Vitali M, Iemma N. Il controllo di qualità della cartella clinica: un ruolo della medicina Legale nelle aziende sanitarie. I criteri e i risultati di una indagine sperimentale. Riv It Med Leg 1997; 19:675-704.
5. Decreto del Presidente della Repubblica 14 gennaio 1997 "Approvazione dell'atto di indirizzo e coordinamento alle regioni e alle province di Trento e di Bolzano, in materia di requisiti strutturali, tecnologici ed organizzativi minimi per l'esercizio delle attività sanitarie da parte delle strutture pubbliche e private".
6. Cassazione Penenale, sez. V, 26.11.1997, in Giust Pen 1999;45:11-25
7. Decreto Ministero della Sanità del 15 dicembre 1986.
8. Ministero della Sanità Dipartimento della Programmazione "Classificazione delle malattie, dei traumatismi, degli interventi chirurgici e delle procedure diagnostiche e terapeutiche" versione italiana della ICD-9-CM (International Classification of Diseases – 9 th revision – Clinical Modification) 1997, Istituto Poligrafico e Zecca dello Stato; Libreria dello Stato 1998.
9. Direzione Generale Sanità, "Classificazione delle malattie, dei traumatismi, degli interventi chirurgici e delle procedure diagnostiche e terapeutiche" vers. italiana della ICD-9-CM (International Classification of Diseases – 9 th revision – Clinical Modification) 2002 Regione Lombadia, novembre 2002
10. AA. VV. Codice della Privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative. Tomo I. Milano, Giuffrè Ed.; 2004.
11. Casiraghi G. Banche di dati, registri e schedari in ambito sanitario. AA. VV. Codice della Privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative. Tomo I. Milano, Giuffrè Ed.; 2004. p 1311-6.
12. Centro Nazionale per L'informatica nella Pubblica Amministrazione. Linee guida per l'utilizzo della firma digitale. http://www.interlex.it/testi/ linguida_fd.htm (data ultima consultazione 22/10/04).
13. Manca G., La firma digitale CNIPA 2003. http://applicazioni.cnipa.gov.it/formazione-firmadig/cnipa_corsi.html (data ultima consultazione 22/10/04).
14. http://www.giustizia.it/cassazione/leggi/dir16gen02.html (accesso riservato).
15. http://www.net-privacy.it (data ultima consultazione 22/10/04).
16. http://www.crs.lombardia.it (data ultima consultazione 22/10/04).