

Le guide di

PRIVACY
E STUDI MEDICI
NEL
TERZO MILLENNIO

PROFESSIONE

Allegato a Doctor n.15 - dicembre 2003 - Sped. in abb. post. - 45% - art. 2 comma 20/B legge 662/96, filiale di Milano



scienze salute



2003 - 2004
P R O F E S S I O N E

PRIVACY E STUDI MEDICI nel TERZO MILLENNIO

L'autore

Mauro Miserendino
è redattore di Corriere Medico, Doctor e Doc Magazine, riviste specializzate per i medici di famiglia dove si occupa in prevalenza di politica sanitaria.

L'opera

Il volumetto intende illustrare i principali cambiamenti che interverranno nello studio del medico di famiglia e del pediatra di libera scelta presumibilmente a partire dal 2004 per l'entrata in vigore del nuovo codice della privacy. Si propone di offrire, se non una descrizione esaustiva della rivoluzione-privacy in sanità e di tutte le situazioni che riguardano il medico, almeno dettagliati rimandi ai principali adempimenti ai quali si dovrà provvedere.

ariete salute Srl

corso Venezia 6
20121 Milano

Direttore responsabile: Silvano Marini
Progetto grafico: Germano Cremonesi
Testi: Mauro Miserendino
Ventilche redazionali: Luciano Lucchini
Stampa: Arti grafiche Nidasio - Assago (MI)

© 2003, Ariete Salute Srl

I diritti dei testi pubblicati in questo fascicolo
sono di proprietà dell'editore.

Nessuna parte può essere ripresa, ristampata o fotocopiata
senza una specifica autorizzazione.

Indirizzi normativi aggiornati al 27-02-2004

Allegato a Doctor n.15 - dicembre 2003 - Sped. in abb. post. - 45%
art. 2 comma 20/B legge 662/96, filiale di Milano

Privacy e studi medici nel terzo millennio

Premessa pag. 6

Segreto, che cosa dice il codice deontologico

Capitolo I pag. 9

Lo scenario della rivoluzione

1.1 - Dal segreto professionale alla legge 675/96

1.2 - Il decreto 318 del 1999

1.3 - Il testo unico in materia di dati personali

1.4 - Che cos'è il trattamento dei dati

1.5 - Dati personali e dati sensibili

Tabelle: quando non occorre chiedere il consenso

1.6 - Autorizzazione e notificazione

Capitolo II pag. 14

Duemilaquattro anno zero

2.1 - Gli articoli 75 e 94

2.2 - Primo gennaio, chiamata per numero

2.3 - Adempimenti di strutture più complesse

2.4 - Primo settembre, si raccoglie il consenso

2.5 - Le ricette irricognoscibili

2.6 - I dati genetici

Capitolo III pag. 19

Come tutelare la riservatezza

3.1 - Diritti dell'assistito e doveri del medico

3.2 - Le misure dell'ex decreto 318

3.3 - Alcune misure particolari

3.4 - I rischi per i medici inadempienti

Tabella riepilogativa delle sanzioni

Capitolo IV pag. 26

Prepararsi al futuro

4.1 - L'evoluzione degli studi medici

4.2 - Trattamento dati per scopi scientifici

4.3 - Trentun marzo, inviare il Dpss

4.4 - Il disciplinare tecnico di sicurezza

Tabella riepilogativa delle incombenze periodiche

Un'ipotesi di modello di consenso

S
o
m
m
a
r
i
o

P r e m e s s a

C'era una volta la legge 675 sulla privacy. Era stata approvata a fine 1996 e istituiva l'Autorità Garante per la Protezione dei Dati Personali, la stessa "authority" che dalla sua nascita è guidata da Stefano Rodotà. L'obiettivo era allineare la legislazione italiana a quella dell'Unione Europea, stabilita con la direttiva 46 del 24 ottobre 1995 sulla libera circolazione dei dati, rafforzando la protezione soprattutto per le informazioni che di sé il cittadino non è disposto a dare a tutti, dall'iscrizione a un partito alla confessione religiosa, dalla salute alla vita sessuale.

In sei anni non solo il nostro paese si è adeguato, ma la legislazione è stata così al passo con i tempi da porre numerosi problemi, spesso sollevati da procedimenti giudiziari: nel 2002 erano circa 30 mila le cause pendenti per presunte violazioni della privacy!

Istruttorie, pronunce, autorizzazioni, normative si sono succedute – insieme a nuove direttive europee come la 2002/58 – in campi disparati, dalla sanità alla giurisprudenza, dal ramo assicurativo alle comunicazioni elettroniche, al punto da rendere indifferibile un testo unico. Testo che – approvato il 30 giugno scorso come decreto legislativo 196, e pubblicato nella Gazzetta Ufficiale del 28 luglio, numero 174 – per semplificare le cose ha abrogato tutte le leggi e i decreti precedenti, inclusa la legge 675. Ne deriva che ha valore di legge e che, se qualche adempimento o sanzione in esso previsti non piacesse ai destinatari, restano due modi per cambiarli: il ricorso in Corte costituzionale (che può fare solo un magistrato nel corso di un processo) o circolari esplicative del Garante volte ad ammorbidire certe norme.

Il codice copre tutto lo scibile del trattamento dei dati. Ma, accanto agli ospedali, saranno i medici di famiglia e i pediatri di libera scelta i professionisti tenuti ad adempimenti burocratici nuovi e spinosi. Il 2004 sarà l'anno della rivoluzione. Tuttavia, anche se il codice prevede come inizio per ogni adempimento il 1° gennaio 2004, il Garante ha di recente assicurato gli ordini dei medici su una tempificazione a tappe per meglio organizzare il sistema. La scansione dei tempi – che cambia la previsione di start al 1° gennaio 2004 dell'articolo 186 del Testo unico – potrebbe essere ancora rivista. Ad oggi prevede che:

Già dal 1° gennaio 2004 medico di famiglia e pediatra di libera scelta devono:

- ~~chiamare gli assistiti in sala d'attesa per numero di arrivo e non più per nome. Nessuno degli astanti deve in teoria poter risalire all'identità dell'altro correlandola con una malattia o uno stato di salute specifico;~~
- mettere in atto comportamenti atti a fare in modo che terzi non colle-

ghino in nessun modo un individuo a una patologia (nessuno nella stanza durante la visita, etc);

- ~~notificarsi al Garante, come dovrebbero sempre aver fatto, per i trattamenti di dati diversi dai compiti di diagnosi e cura;~~
- far aderire i loro documenti programmatici sulla messa in sicurezza dei dati sensibili, prodotti ogni 31 marzo dell'anno, alle regole imposte dall'allegato B al testo unico (vedi ultimo capitolo).

~~Dal 30 settembre 2004, se il Garante non affiderà l'incombenza burocratica agli sportelli delle Asl, generalisti e pediatri dovranno:~~

- raccogliere il consenso (sì o no) di ogni proprio assistito al trattamento dei suoi dati personali consegnando un'informativa in cui si specifica che tale consenso verrà esteso ai sanitari con i quali il paziente verrà via via in contatto; in particolare il sostituto e il collega associato, ma anche lo specialista interpellato dal curante in ospedale o sul territorio, nel pubblico o nel privato, e il farmacista;
- annotare la risposta – sì o no – accanto alla data in cui è stata raccolta; secondo il codice non c'è bisogno della firma dell'assistito ma non è impossibile che circolari contrattate con gli ordini impongano un consenso firmato a tutela dei medici;
- collocare un adesivo sul libretto o tessera sanitaria dell'assistito attestante che l'assistito stesso acconsente o meno a che i propri dati siano trattati dal proprio medico e da altri sanitari.

Dal 1° gennaio 2005 arriveranno le nuove ricette anti-intruso. Medici e pediatri dovranno:

- criptare le prescrizioni di farmaci, visite ed esami sui ricettari del servizio sanitario regionale apponendo un bollino adesivo sulle generalità dell'assistito, che il medico dovrà comunque scrivere;
- ~~non scrivere il nome del proprio assistito sulle prescrizioni di farmaci, visite ed esami sul ricettario bianco che non sono a carico del Servizio sanitario nazionale,~~ così che nessuno possa leggere sullo stesso foglio nome della patologia e suo portatore.

Questa la rivoluzione in sintesi. Ma già dal '96 i medici di famiglia sarebbero tenuti, in base alla legge 675, a raccogliere il consenso dei propri assistiti al trattamento dei loro dati sensibili, e dal 2000 devono redigere ogni anno un documento programmatico sulla sicurezza dei dati. Vale perciò la pena di riepilogare le principali tappe vissute negli studi, rivisitare il significato di qualche termine e quindi focalizzare vecchi e nuovi adempimenti.

SEGRETO CHE COSA DICE IL CODICE DEONTOLOGICO (1999)

Articolo 9 - Segreto professionale

Il medico deve mantenere il segreto su tutto ciò che gli è confidato o che può conoscere in ragione della sua professione; deve, altresì, conservare il massimo riserbo sulle prestazioni professionali effettuate o programmate, nel rispetto dei principi che garantiscano la tutela della riservatezza.

La rivelazione assume particolare gravità quando ne derivi profitto, proprio o altrui, o nocumento della persona o di altri.

Costituiscono giusta causa di rivelazione, oltre alle inderogabili ottemperanze a specifiche norme legislative (referti, denunce, notifiche e certificazioni obbligatorie):

a) la richiesta o l'autorizzazione da parte della persona assistita o del suo legale rappresentante, previa specifica informazione sulle conseguenze o sull'opportunità o meno della rivelazione stessa;

b) l'urgenza di salvaguardare la vita o la salute dell'interessato o di terzi, nel caso in cui l'interessato stesso non sia in grado di prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere e di volere;

c) l'urgenza di salvaguardare la vita o la salute di terzi, anche nel caso di diniego dell'interessato, ma previa autorizzazione del garante per la protezione dei dati personali. La morte del paziente non esime il medico dall'obbligo del segreto.

Il medico non deve rendere al giudice testimonianza su ciò che gli è stato confidato o è pervenuto a sua conoscenza nell'esercizio della professione. La cancellazione dall'albo non esime moralmente il medico dagli obblighi del presente articolo.

Articolo 10 - Documentazione e tutela dei dati

Il medico deve tutelare la riservatezza dei dati personali e della documentazione in suo possesso riguardante le persone anche se affidata a codici o sistemi informatici. Il medico deve informare i suoi collaboratori dell'obbligo del segreto professionale e deve vigilare affinché essi vi si conformino.

Nelle pubblicazioni scientifiche di dati clinici o di osservazioni relative a singole persone, il medico deve assicurare la non identificabilità delle stesse. Analogamente il medico non deve diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire l'identificazione del soggetto cui si riferiscono.

Articolo 11 - Comunicazione e diffusione di dati

Nella comunicazione di atti o di documenti relativi a singole persone, anche se destinati a Enti o Autorità che svolgono attività sanitaria, il medico deve porre in essere ogni precauzione atta a garantire la tutela del segreto professionale. Il medico, nella diffusione di bollettini medici, deve preventivamente acquisire il consenso dell'interessato o dei suoi legali rappresentanti.

Il medico non può collaborare alla costituzione di banche dati sanitari, ove non esistano garanzie di tutela della riservatezza, della sicurezza e della vita privata della persona.

Lo scenario della rivoluzione

Dalla legge 675 al decreto sulla messa in sicurezza dei dati, ecco come si è evoluta la tutela del "dato sensibile"

1.1 - Dal segreto professionale alla legge 675/96

Il 31 dicembre 1996 è promulgata la legge 675 sulla tutela della privacy. Essa prescrive che il medico non può rivelare lo stato di salute del suo paziente senza il consenso di quest'ultimo. Non può rivelarlo a nessuno, nemmeno ai parenti. Il divieto va a integrarsi con gli articoli 326 e 622 del codice civile che da 70 anni impongono al medico il segreto professionale. Gli unici due casi in cui non si deve chiedere il permesso al paziente si verificano quando il medico ha scoperto che è affetto da una malattia contagiosa e ritiene di doverlo rivelare per tutelare la vita o l'incolumità dei suoi familiari o di terzi.

Analoghe previsioni sono nel codice di deontologia medica rinnovato, che ammette l'informazione ai congiunti quando il paziente lo consente per la salvaguardia della vita di terzi o perché c'è un'imposizione di legge. Per il resto, il medico deve tutelare la riservatezza della documentazio-

ne in suo possesso riguardante i pazienti, deve garantire la segretezza nella compilazione e trasmissione di ogni atto, deve assicurarsi della tutela della riservatezza se collabora alla costituzione di banche dati sanitarie (articoli 9, 10, 11).

Peraltro, a differenza di altre imprese ed operatori, che necessitano di autorizzazione del Garante conseguibile previa richiesta, il medico può trattare dati (sensibili) inerenti alla salute e alla vita sessuale del suo assistito in quanto esercente professioni sanitarie in base all'autorizzazione del 27 novembre del '97. Certo, non può farlo per tutte le attività, ma solo per fini di diagnosi e cura, di ricerca o amministrative interne.

Ciò non toglie che per trattare i dati dell'assistito il medico non sia dispensato dal chiedere il consenso all'interessato. In caso di mancato consenso con fuga di notizie e danni rischia anche anni di reclusione, e di dover risarcire cifre ingenti.

Il consenso al trattamento in teoria in questi anni doveva essere

rinnovato ogni volta che, anziché il proprio medico di fiducia, il paziente si trovava di fronte un suo sostituto. Ad oggi non ci sono cifre su quanti generalisti abbiano chiesto tale consenso e su come lo abbiano fatto. D'altronde, il Garante negli ultimi anni ha seguito una linea morbida preferendo il dialogo ai controlli e alle sanzioni a tappeto. Tranne in un caso.

1.2 - Il decreto 318 del 1999

Il 26 luglio 1999 esce il decreto 318 sulle misure di sicurezza da adottare per proteggere i supporti contenenti dati sensibili, conforme alla direttiva 95/46 dell'Unione Europea.

Entro il 1999 i medici di famiglia e i pediatri di libera scelta avrebbero dovuto notificare al Garante i loro dipendenti e collaboratori incaricati del trattamento dei dati personali dei pazienti e della manutenzione dei dati. Contestualmente, in un documento annuale (documento programmatico) avrebbero dovuto definire criteri organizzativi per proteggere aree e locali, procedure per assicurare l'integrità dei dati e la sicurezza della loro trasmissione, programmi di formazione per il personale. Tempo per presentare il documento al Garante: fine 1999; tempo per mettersi in regola, primavera del 2000. Ma nel marzo del

2000 arriva un'altra legge, la 315, che proroga a tutto il dicembre di quell'anno il tempo per mettersi in regola, riservando però il diritto solo a chi ha presentato il documento programmatico sulle misure di sicurezza.

Da allora sono successe varie cose. I casi giurisprudenziali – in particolare il processo di Cremona alle cooperative di medicina generale – hanno evidenziato che non esistono criteri di messa in sicurezza inattaccabili e che i dati dei medici, soprattutto quando si lavora in gruppo con computer collegati in rete, sono sempre più o meno esposti ad occhi indiscreti.

Il Garante ha preso atto di simili difficoltà e da parte sua ha proceduto a una semplificazione delle normative; nel contempo però ha preso atto che in alcuni casi la normativa creava intoppi. Pensiamo alla difficoltà per i medici a trasmettersi i dati di un paziente se questi non ha espresso consenso esplicito al loro trattamento; o al paziente ricoverato all'insaputa dei parenti che lo cercano e alla successiva reticenza – per non infrangere le regole – della struttura che lo ha in cura.

L'Autorità ha chiesto così all'ordine dei medici di contrattare una richiesta di consenso al trattamento dei dati che, sin dal

momento della sua accettazione da parte del malato, lo rendesse implicito. Il consenso, nelle intenzioni del Garante, andava raccolto proprio dai medici di famiglia, quegli stessi che già dal '97 avrebbero dovuto raccogliere il sì o il no di ogni assistito al trattamento dei suoi dati, ma questa volta avrebbe dovuto estendersi a tutti gli altri sanitari che prima o poi avessero avuto in cura quel paziente. Dopo tre anni di trattative con sindacati medici e ministro della Salute, ecco il Testo unico.

1.3 - Il testo unico

È anche chiamato "Codice della privacy", è diviso in tre parti (disposizioni generali, settori specifici, applicazione) e non si occupa solo di sanità, ma anche di dati giudiziari, polizia, pubblica amministrazione, istruzione, lavoro, banche e assicurazioni, comunicazioni elettroniche, investigazione privata, giornalismo e marketing diretto.

Il Garante sottolinea alcune novità. In passato, ad esempio, chiunque trattasse dati di cittadini doveva notificarsi al Garante, ora la notifica va effettuata solo se si trattano dati sensibili, o nel campo della profilazione dei consumatori.

Vengono semplificate le procedure di richiesta di consenso per le banche, viene data facoltà

a una parte in un processo a che il suo nome sia tolto in caso di pubblicazione della sentenza su riviste giuridiche; si dettano regole per redigere le liste di collocamento; sono prolungate al 30 giugno 2004 le autorizzazioni a trattare dati sensibili e giudiziari, si prevedono codici deontologici per il trattamento dei dati su Internet, videosorveglianza, direct marketing.

In sanità vengono rivoluzionati i criteri di accettazione in studi, ambulatori, ospedali, in modo da non ricollegare un paziente a una malattia. Vengono previste modalità di raccolta specifiche a fini di ricerca o catalogazione dei dati genetici. Quanto alla diagnosi e cura, sono codificati nello studio del medico informativa e consenso.

Il testo originale prevede che l'obbligo di raccolta negli studi parta da gennaio 2004, ma il Garante ha dato rassicurazione alla Federazione degli ordini che si partirà a settembre, dopo che sarà stato risolto come rendere esplicito il sì del paziente sulla sua tessera. E, sempre per la necessità di predisporre adeguati sistemi di criptazione dei dati personali sulla ricetta, slitterà al gennaio 2005 la prescrizione di farmaci, esami e visite specialistiche.

Prima di focalizzare le innovazioni del codice relative agli adem-

pimenti dei medici di primo livello, occorre tuttavia fare un po' di chiarezza sulla definizione di trattamento e sulla differenza esistente tra dati personali identificativi e dati sensibili e differenziare anche in quest'ultima categoria i dati sensibili sanitari da quelli non sanitari.

1.4 - Che cos'è il trattamento dati

Per trattamento dei dati (articolo 4 comma 1a) si intendono diciassette procedimenti che una persona interessata, medico incluso, può fare avendo in mano riferimenti di singoli cittadini (anche non registrati in un archivio computerizzato, ma ad esempio in una semplice agenda telefonica): raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione.

Ma quali sono i dati in questione, oggetto di trattamento?

1.5 - Dati personali e dati sensibili

Nome, cognome, indirizzo, sono dati importanti, che a nessuno piacerebbe dare in pasto al pubblico. Ma ci sono altri dati, detti "sensibili", perché al cittadino interessano in misura maggiore: pensiamo a quelli che indicano la confessione religiosa o la fede politica, o l'iscrizione a un sinda-

cato. Tali dati (elencati all'articolo 4 comma 1d) non possono essere oggetto di trattamento al di fuori delle organizzazioni (sindacati, partiti, chiese) che per legge li trattano, i quali però possono raccoglierti anche senza il consenso dell'interessato.

Per tornare al medico, sono dati sensibili quelli riferiti a salute e sfera sessuale, sui quali da sempre va tenuto il segreto professionale. Questo rispetto a terzi; ma rispetto a sanitari che possono salvare la vita al paziente? Per il codice della privacy, i dati sensibili possono essere "girati" senza consenso (articolo 24) se ci sono motivi di interesse pubblico o la salvaguardia di terzi. Non possono mai essere diffusi. Possono essere trasmessi adempiendo a norme europee in particolari casi dov'è in gioco l'igiene e la sicurezza sul lavoro o della popolazione.

I dati non sensibili/identificativi possono essere trattati lecitamente senza consenso, sempre per fini correlabili all'attività sanitaria, in alcuni casi comunque correlati alla tutela della salute e riportati nella tabella a fianco.

1.6 - Autorizzazione e notificazione

Con autorizzazione generale ad hoc, i medici sono stati esentati dal Garante dal chiedergli il permesso a trattare i dati dei pazienti non solo per finalità di dia-

gnosi e cura ma anche per fini di ricerca. Ciò non toglie che, accanto a raccolta di consenso e obblighi di messa in sicurezza dei dati con compilazione di documento programmatico, ~~c'è un altro adempimento: la notificazione (articolo 39) del trattamento particolare di dati personali.~~ Tale adempimento riguarda tutti i medici coinvolti in ricerche genetiche che rendano riconoscibili/rintracciabili i nominativi inseriti, sia soprattutto in operazioni a fini di:

- procreazione assistita;
- prestazioni sanitarie svolte via Internet (banche dati);
- indagini epidemiologiche;

- rilevazione di malattie mentali, infettive e diffuse;
- sieropositività all'Hiv;
- trapianto di organi e tessuti;
- monitoraggio della spesa sanitaria.

Per chi fosse interessato a tali attività, la notificazione si presenta al garante prima dei lavori di trattamento e una sola volta a prescindere dal numero di operazioni svolte, su modello telematico apposito, e si ripresenta prima di cessare il trattamento o di cambiare elementi della notificazione precedente.

A lavorare ad un trattamento si inizia dopo 45 giorni dall'ok del Garante.

QUANDO NON OCCORRE CHIEDERE IL CONSENSO

NELL'AMBITO DEL SSN

Operazioni di trattamento dati sensibili nell'ambito del Ssn per le quali è permesso non chiedere il consenso all'interessato (articolo 85)

- Prevenzione, diagnosi e cura
- Attività correlate alle precedenti
- Gestione dei flussi dei dati sull'assistenza sanitaria
- Farmacovigilanza
- Certificazioni
- Verifica di igiene e sicurezza dei luoghi di lavoro
- Collegamento tra enti del Ssn o tra singoli sanitari (previo consenso al medico di famiglia)

FUORI DAL SSN

Operazioni di trattamento dati sensibili anche effettuate all'esterno del Ssn per le quali è permesso non chiedere il consenso all'interessato (articolo 86)

- Tutela della maternità
- Interruzioni di gravidanza
- Assistenza a tossicodipendenti
- Gestione di comunità alloggio, assegni ed istruzione a portatori di handicap

2.1 - Gli articoli 75 e 94

A entrare nello specifico della sanità è il titolo V del codice della privacy, con gli articoli dal 75 al 94. Dal testo, abbiamo estratto gli adempimenti richiesti ai medici di famiglia e ai pediatri di libera scelta nell'ordine in cui, secondo gli ultimissimi indirizzi del Garante, dovrebbero comparire. Tuttavia da gennaio 2004, pare ormai certo, entrerà in vigore un altro obbligo in sostanza molto oneroso. Si tratta di far rispettare alcune misure di sicurezza, valide sia per i generalisti sia per gli altri medici (dagli specialisti agli ospedalieri dipendenti di strutture pubbliche e private), atte a tutelare il segreto circa la salute dei pazienti.

2.2 - Primo gennaio, chiamata per numero

~~La misura chiave è all'articolo 83 ("Altre misure per il rispetto dei diritti degli interessati") e richiede di non chiamare mai i propri assistiti per nome quando aspettano il loro turno in sala d'attesa. L'articolo prescrive che quando si chiama la persona, cui si sta per erogare una qualsiasi pre-~~

Dal sì al trattamento dei dati sensibili valido per altri sanitari alle ricette "bendate": ecco le novità dal prossimo anno

~~stazione (dalla terapia alla sua semplice prescrizione) o adempimento amministrativo (certificazione), si deve seguire l'ordine di presentazione "prescindendo dall'individuazione nominativa". Per meglio adeguarsi, gli studi medici potrebbero dotarsi di macchinetta "sputa numero" per cui ogni paziente, entrando in sala d'attesa, ritirerebbe il proprio in ordine progressivo, come già si fa, ad esempio, nei laboratori di analisi cliniche. Potrebbe inoltre crescere potenzialmente il rapporto del medico di famiglia con l'ospedale. Per l'articolo 84 sarà un medico di fiducia a recuperare i dati dell'assistito detenuti dagli ospedali in cui questi è stato ricoverato: «I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai congiunti da parte di esercenti le professioni sanitarie solo per il tramite di un medico designato dall'interessato o dal titolare a meno che quei dati non siano stati in precedenza forniti all'interlocutore dall'interessato stesso». Terza regola che riguarda gli studi dei generalisti come gli~~

ospedali: tutti gli incaricati del trattamento dati sensibili (infermieri, collaboratori di studio) andranno sottoposti alle regole sul segreto professionale.

2.3 - Adempimenti di strutture più complesse

L'articolo 83 chiede altri adempimenti, stavolta più tagliati, verso strutture complesse come le accettazioni degli ospedali e gli sportelli Asl. Intanto, ci vorranno distanze e barriere salva-privacy agli sportelli; quindi, si chiede che la raccolta di dati sanitari non avvenga di fronte a terzi non aventi interesse "specifico e preminente" a conoscere la salute dell'interessato. Ancora, occorrerà rispettare la dignità dell'interessato in ogni operazione di trattamento dei dati (è capitato in alcune sale d'attesa che portatori di malattie diverse siano stati chiamati ciascuno per il nome della malattia o della prestazione specifica da erogare). Le stesse liste d'attesa nel caso pratico non dovrebbero più essere nominative. Seguono tre norme pratiche per le corsie. Se un paziente viene ricoverato in una struttura e non può o non vuole vietare che ciò si sappia, occorre assicurare ai terzi interessati l'informazione relativa al suo ricovero. Sempre dopo avere informato il ricoverato e averne ottenuto il consenso, è necessario dire esattamente

dove si trova il paziente ai parenti che vanno a visitarlo. Infine, sarà bene tenere il più allentata possibile, di fronte a estranei, la correlazione tra ricoverati e loro stato di salute.

2.4 - Trenta settembre, si raccoglie il consenso

L'adempimento più nuovo e oneroso per il medico di famiglia è all'articolo 78. ~~Dal 30 settembre 2004 (è la scadenza annunciata dal Garante alla Federazione degli ordini), a meno che l'incombenza non sia affidata alle Asl, generalisti e pediatri dovranno chiedere il consenso degli assistiti per trattare i loro dati sensibili; il "sì" servirà per poterli girare anche ad altri professionisti della sanità quando necessario. Il consenso andrebbe raccolto man mano che gli assistiti si presentano nello studio, a partire appunto da settembre 2004. La procedura in esame, prevista per motivi di diagnosi e cura, è in forma semplificata e consta di un'informativa, della domanda e risposta (richiesta del consenso) e dell'annotazione della risposta. In extremis, come vedremo, potrebbe essere introdotta anche la firma del paziente.~~

a) L'informativa pre-consenso
L'informativa (articolo 13) è la spiegazione da parte del medico dei motivi per i quali serve la raccolta del consenso.

Si dirà all'assistito che altri sanitari, in particolare se interpellati dal curante stesso, potranno conoscere i suoi dati sanitari per motivi di prevenzione, diagnosi, cura nei suoi confronti.

Il curante dovrà contestualmente informare l'assistito del fatto che può anche negare il consenso alla possibilità di conferire i propri dati ad altri medici, ma nel contempo gli dovrà ribadire che il suo "no" potrebbe creargli gravi difficoltà. E' disagevole dover prestare il consenso ogni volta che ci si fa visitare da un medico o, peggio, non poter essere curati in certe situazioni di emergenza in cui non ci si ricorda, ad esempio, alcuni dettagli circa le cure effettuate o in atto. Il medico dovrà poi dire in quali mani potrebbero andare questi dati, per esempio epidemiologi e ricercatori che studiano l'incidenza di certe malattie sulla collettività. Preferibilmente, le informative saranno fornite prestampate. Il codice parla di "carte tascabili con allegati pieghevoli" dove ne vengono riepilogati motivi e punti. E' chiaro che dovranno essere messe a punto dalle pubbliche amministrazioni e che la difficoltà per adeguarsi è all'origine dello slittamento della scadenza e del ventilato affidamento dell'onere agli sportellisti Asl.

b) I destinatari del consenso

Dall'informativa si è dispensati

solo se richiede impiego sproporzionato di mezzi o se i dati sono trattati in base a obblighi di legge o per tutelare un diritto sancito in sede giudiziaria.

Ma chi sono i destinatari dei dati inoltrabili dal medico una volta ottenuto il consenso? Si tratta:

- dei sostituti del medico di famiglia o del pediatra;
- degli specialisti interpellati da medico e pediatra;
- dei loro colleghi associati ai quali può capitare di sostituirli;
- dei farmacisti "chiamati in causa" dalla ricetta;
- di tutti i professionisti – o soggetti indicati dalla normativa, non necessariamente sanitari (e dunque collaboratori di studio e segretari) – che entrano in contatto con il medico di famiglia o il pediatra per fornirgli a loro volta dati sui suoi assistiti (articolo 79). Anche gli ospedali pubblici e privati, titolari di personalità giuridica, possono avvalersi delle modalità semplificate di raccolta del consenso che sarà estensibile a cascata a tutti i reparti con cui il paziente potrà entrare in contatto, ma dovranno avere organismi di sorveglianza del processo di raccolta dati (articolo 80).

c) Il consenso vero e proprio

E veniamo al "sì" del paziente. E' semplificato, in quanto basta che sia verbale. Inizialmente il Garante ha proposto che il medico

dovesse semplicemente annotarlo, scrivendo accanto la data di avvenuta registrazione. Ma la norma non era ancora del tutto codificata che i medici avevano obiettato la pericolosità di una tale formula. Infatti, nulla dimostrerebbe che il paziente ha dato l'assenso e, in caso di contenzioso, quest'ultimo potrebbe dire che il medico si è inventato il consenso. In una recente riunione con il Garante gli ordini dei medici hanno ottenuto di poter sperimentare (sempre dal 30 settembre 2004) il consenso scritto: il paziente dovrebbe dunque firmare il permesso al suo curante di detenere i dati sensibili contenuti nella sua scheda personale. E' probabile che la modalità scritta, come previsione, si estenda entro fine 2003 a tutto il consenso.

d) Bollini sui libretti sanitari

Secondo problema: come far sapere a tutti i professionisti che vengono in contatto con l'assistito per scopi di prevenzione, diagnosi e cura che questi è favorevole a che si conoscano i suoi dati di salute? Il garante pensa di introdurre per settembre 2004 un bollino da applicare o consegnare ai medici o, in alternativa, da far consegnare agli utenti allo sportello Asl affinché sia incollato sulla vecchia tessera sanitaria o sulla futura carta sanitaria elettronica.

e) Dispensa dal consenso

E se l'assistito finisse in ospedale in coma prima che si sappia se è favorevole o no al trattamento dei propri dati?

In tal caso, informativa e consenso possono – sancisce il Garante all'articolo 82 – intervenire successivamente alla prestazione (casi di emergenza sanitaria/igiene). Il medico si può comportare allo stesso modo se c'è di mezzo un bambino per il quale non sia possibile acquisire il consenso da genitori, familiari o da chi esercita legalmente la patria potestà o se si presenti rischio grave, imminente e irreparabile per la sua salute. Dopo il raggiungimento della maggiore età, il procedimento della raccolta di consenso previa informativa si ripeterà.

Infine, ma solo per salvaguardare terzi e collettività in casi particolari (ad esempio per gravi malattie contagiose), i sanitari potranno, come previsto sin dal 1996, evitare di chiedere il consenso a un trattamento e girare i dati ai colleghi interessati (ma in quest'ultimo frangente serve la preventiva autorizzazione del Garante, onere dal quale si è dispensati in tutti gli altri casi).

2.5 - Le ricette irriconoscibili

I sindacati dei medici di famiglia non vogliono sentirne parlare, ma l'articolo 87 parla chiaro: dal 1° gennaio 2005 ogni volta che

il medico (o il pediatra) compila una ricetta, per ogni assistito destinatario di una prescrizione a carico del Ssn dovrà apporre una fascetta adesiva o un tagliando sul foglietto del servizio sanitario regionale così da rendere irriconoscibili i destinatari della terapia o dell'impegnativa a farmacisti e agli altri sanitari.

Il tagliando tuttavia potrà essere momentaneamente staccato dal medico dell'Asl autorizzato a effettuare verifiche amministrative, contabili o di appropriatezza della prescrizione. Anche il farmacista (articolo 87 comma 4), per verificare la correttezza di un'operazione, può staccare occasionalmente il tagliando annotando però l'operazione sulla ricetta e controfirmando in calce.

~~Il Garante chiede poi di non indicare le generalità per i farmaci non a carico del servizio sanitario, vale a dire quelli che il paziente pagherà per intero (articolo 88) a fronte della presentazione della ricetta "bianca" intestata al proprio curante.~~

I medici hanno fatto presente che tale indicazione – prevista comunque anch'essa dal gennaio 2005 – favorirà confusioni e impedirà agli assistiti di scaricare il costo dei farmaci dalla dichiarazione dei redditi.

L'indicazione delle generalità è ammessa soltanto in casi indispensabili (articolo 89), come

l'urgenza che il farmacista dispensi al malato una particolare preparazione in passato già somministratagli.

Sono esclusi dalla disciplina gli stupefacenti per la cui prescrizione va sempre accertata l'identità del malato (dpr 309/90) e per i quali la ricetta del curante va conservata in un archivio separato.

2.6 - I dati genetici

In base all'articolo 90 del codice, da gennaio 2004 per girare ad altri i risultati di test genetici occorre l'autorizzazione del Garante che nell'assenso, previo placet del ministero della Salute e del Consiglio superiore di sanità, specificherà che cosa si può fare con quei dati. Di recente i garanti europei hanno detto no ai test genetici sul lavoro e chiesto regole ferree per la schedatura dei dati biometrici dei lavoratori (altezza, peso, etc). In estate, il presidente dell'Autorità garante Stefano Rodotà in un articolo ha ricordato i rischi potenziali derivanti dalla schedatura dei dati genetici: negli Stati Uniti le donne rinunciano ai test predittivi di tumore alla mammella per timore che le assicurazioni sappiano della predisposizione ad ammalarsi e annullino le polizze salute. Tornando al codice, sempre all'articolo 90, i donatori di midollo osseo hanno diritto-dovere di mantenere l'anonimato nei confronti di terzi.

Come tutelare la riservatezza

3.1 - Diritti dell'assistito e doveri del medico

T trattare i dati della gente non è mai così indispensabile. O meglio, il trattamento è un'eccezione alle normali regole quotidiane che prevedono l'uso della massima discrezione da parte di chi detiene dati personali.

Si potrebbe interpretare così il principio generale (internazionale) di necessità del trattamento dei dati (sensibili e non; articoli 18-22) che esclude il suddetto trattamento quando le finalità perseguite possano essere realizzate con dati anonimi o coperture che rendano l'interessato identificabile soltanto in caso di necessità. Inoltre l'oggetto del trattamento "non deve eccedere le finalità" e i dati vanno conservati in forma che consenta di identificare l'intervento per un tempo non eccedente l'espletamento degli scopi della raccolta. All'articolo 12, il Garante promuove dei codici di buona condotta per chi nei vari ambiti, sanità inclusa, tratti i dati personali. L'assistito in particolare ha diritto a sapere se la tal banca, come il tal medico, possiedano o meno i suoi dati e, in caso posi-

Il generalista resta obbligato ad archiviare in tutta sicurezza i dati degli assistiti, altrimenti incorrerà in sanzioni penali

tivo, a sapere chi ha consegnato i suoi dati perché, come vengono usati, come sono protetti, chi è deputato alla protezione, chi può venire in possesso di tali informazioni. Può ottenere aggiornamenti e rettifiche, ma anche la cancellazione.

Può comunque opporsi:

- *per motivi legittimi*, al trattamento dei propri dati anche se fosse pertinente lo scopo della raccolta (cioè utile pure a lui);
- *sempre*, al trattamento degli stessi dati se compiuto al fine di inviargli materiale commerciale pubblicitario o per effettuare ricerche di mercato.

Per far cessare il trattamento ci si deve rivolgere per iscritto o inviando una raccomandata o un'e-mail al *titolare* o al *responsabile*; in caso di rilascio delle cartelle cliniche si può trattare con *l'incaricato*.

Chi sono queste tre figure?

Il titolare del trattamento (articolo 28) è l'intestatario della struttura; il medico di famiglia o il pediatra titolare dello studio; l'ente ospedaliero stesso se questo ha personalità giuridica; l'amministrazione dell'Asl.

Il responsabile (articolo 29)

nello studio convenzionato è ancora il medico di famiglia; nell'associazione, mentre i titolari sono in genere tutti medici associati, i responsabili dovrebbero essere tutti i colleghi del titolare che vengono in contatto con i dati dell'assistito (in realtà il codice si ferma a dire che dovrebbe essere responsabile qualunque individuo capace di far funzionare il sistema informatizzato).

L'*incaricato* (articolo 30) può essere un semplice addetto con funzioni di segreteria avente accesso all'archivio in determinate situazioni, che lavora sotto la diretta autorità del titolare o del responsabile del trattamento.

Il titolare dello studio deve agevolare l'accesso ai dati personali dell'interessato e semplificare le modalità e i tempi di riscontro. Può comunicare i dati anche verbalmente o mostrarli all'utente in video, stamparli, trasmetterli e, se il caso, consegnarne copia.

Se i dati fanno parte di elenchi leggendo i quali l'assistito verrebbe a sapere segreti di altri assistiti, il medico non deve consegnare la documentazione completa a meno che sia impossibile comprendere i contenuti di essa. Per coprire eventuali costi delle pratiche richiestegli può chiedere all'assistito un rimborso spese entro 15 giorni.

Quando il medico non è più curante (cessazione del trattamento), i dati del paziente posso-

no essere ceduti al titolare che subentra nell'ambito di un trattamento compatibile con il precedente, e cioè il nuovo medico curante. In pratica all'adempimento dovrebbe provvedere l'Azienda sanitaria locale.

I dati sensibili possono altresì essere conservati dal curante a soli fini personali, ad esempio per tutelarsi entro un certo periodo in caso di denuncia per patologia che l'assistito dichiarasse insorta o peggiorata in seguito a errore od omissione del medico.

Possono infine essere distrutti.

Non devono essere diffusi, ma possono essere forniti ad altri titolari di trattamento autorizzati per scopi storici, statistici e scientifici.

3.2 - Le misure dell'ex decreto 318

Il decreto 318 del 1999 ora abrogato, oltre all'incombenza del documento programmatico sulla sicurezza (Dpss) da spedire ogni anno al Garante, ha introdotto una disciplina "ferrea" per la conservazione dei dati negli studi medici. Gli adempimenti si differenziano a seconda se lo studio è gestito su base cartacea o è informatizzato.

Negli studi dove le schede degli assistiti si raccolgono su carta (articolo 35) va approntata una tipologia di custodia paradossalmente più complicata (armadio delle schede-assistito chiuso a

chiave; chiavi consegnate agli incaricati solo in certi frangenti; armadio o schedario dedicato alla custodia di ricette per gli stupefacenti). E la custodia – è intuitibile – diventa complicatissima in caso di gestione di gruppo.

Per gli studi informatizzati (articolo 36) il codice oggi parla di "adozione di procedure di gestione delle credenziali di autenticazione".

Prefigurando l'ampio uso della rete nelle medicine associate, si parla poi di utilizzo di sistemi di autorizzazione del medico al trattamento: in un'associazione tutti i medici sono responsabili dei dati degli assistiti con cui (anche sporadicamente) entrano in contatto, e ricevono dal collega, titolare di ogni singolo elenco, un identificativo e una password.

I mansionari degli incaricati vanno aggiornati periodicamente, e gli strumenti elettronici vanno potenziati per difendersi da intrusioni illecite.

E ancora: devono essere adottate procedure per la custodia di copie di sicurezza, va tenuto un documento programmatico sempre sulla sicurezza, e si devono adottare codici cifrati per il trattamento di dati che potrebbero rivelare patologie o disfunzioni sessuali di questo o quell'assistito.

Per più dettagliate delucidazioni rimandiamo all'allegato B al decreto (capitolo IV).

3.3 - Alcune misure particolari

Ci sono poi situazioni che fanno parte del rapporto tra medico di famiglia e ospedaliero.

Di seguito riportiamo tre casi.

- **Cartelle cliniche** (articolo 92). Il signor Rossi va in un poliambulatorio per un esame per il quale va aperta una cartella clinica. Di quella cartella tornerà in possesso o personalmente o attraverso il suo medico di fiducia (all'articolo 83 si parla in realtà di medico da lui designato) per quanto lo riguarda. Se altri volessero accedere alla cartella del signor Rossi (o averne copia) la risposta del medico o dell'incaricato dell'amministrazione dovrà essere ferma e negativa, a meno che non vi sia un'autorizzazione del giudice in seguito a procedimento atto a far valere un diritto di terzi; diritto di rango pari alla privacy dell'interessato (personale o relativo a libertà fondamentale).

- **Madri e figli** (articolo 93). In un reparto di ostetricia dal gennaio 2004 si dovranno seguire regole ancora più strette. Intanto, i dati della madre vanno separati da quelli di eventuali nascituri, il che implica due cartelle distinte e custodite in comparti diversi.

Ancora: il certificato di assistenza al parto va tenuto distinto dall'attestazione di nascita da rilasciare per i registri anagrafici. Se una madre non riconosce il figlio i suoi dati possono essere

rilasciati a chi ne ha interesse dopo cento anni, o in alternativa senza rendere identificabile la donna.

• **Trasferimento dati all'estero** (articoli 42-45).

Poniamo che data la rarità, specificità o gravità della sua malattia un cittadino italiano decida di curarsi all'estero. La legge non pone alcuna difficoltà al trasferimento da strutture italiane ad altre straniere con il consenso del paziente. E del resto, dal 2005 ci si dovrebbe poter curare in ogni angolo dell'Unione europea con gli stessi diritti.

Secondo il codice, in caso di epidemie (si pensi alla Sars) un ospedale può trasferire tutti i dati personali e sensibili di un ricoverato in un paese dell'Unione europea (senza bisogno del suo consenso) per informare le autorità sanitarie competenti, a salvaguardia della vita o dell'incolumità fisica di terzi o della collettività.

In tutti gli altri casi, prima di trasferire le informazioni, a meno che non siano ricavabili da documenti amministrativi accessibili a tutti, è necessario che il titolare del trattamento chieda il consenso al paziente.

Se la commissione dell'Unione europea lo dovesse autorizzare, il trasferimento dati sarebbe possibile anche verso paesi che non facciano parte della comunità europea.

3.4 - I rischi per i medici inadempienti

L'inadempimento agli obblighi imposti dal testo unico a chi tratta i dati sensibili dei pazienti comporta sia sanzioni amministrative sia sanzioni penali. Prevede anche la possibilità di pendenze civili.

- Le *sanzioni amministrative* saranno probabilmente le più ricorrenti, poiché riguardano violazioni per il medico il quale dimenticasse (da settembre 2004) di chiedere il consenso.

Che cosa succede se il medico immagina di aver raccolto un consenso mentre il paziente gli ha risposto no? In realtà l'ipotesi non è campata in aria: un

paziente può negare di essere stato informato dal medico sull'esistenza di un trattamento che lo riguarda. Argomento tanto più facile da far valere in quanto il consenso al trattamento dati negli studi è rilevato verbalmente. In tal caso (omessa informativa) il medico rischia di dover sborsare fino a 18 mila euro (30 mila per trattamenti di dati sensibili che mettano a rischio le libertà fondamentali), e la somma può crescere in proporzione alla ricchezza.

Secondo caso: se il medico (dal 1° gennaio 2004) chiamando un paziente per nome ne rende riconoscibile la patologia o il semplice stato di salute a rischio può configurarsi a suo carico una

cessione di dati ad esercente non interessato a conoscerli: rischia, ancora una volta, fino a 30 mila euro di sanzione.

Terzo caso: se un paziente viene a sapere di cose che riguardano la sua salute da persona non titolata né indicata da lui (o dall'ospedale), il titolare dello studio o il medico che in quel caso lo ha sostituito, se citati in giudizio dall'interessato, rischiano fino a 3 mila euro di ammenda.

- E veniamo alle *sanzioni penali*. Si entra decisamente in campo penalistico se, invece, il medico si dimentica i dati del paziente sotto gli occhi di tutti, ad esempio lasciando le schede cliniche degli assistiti sulla scrivania.

SANZIONI AMMINISTRATIVE

TIPOLOGIA	ARTICOLO	PENA PECUNIARIA	PENA ACCESSORIA
Omessa o inidonea informativa	161	euro 3.000-18.000	triplicabile in base al reddito del destinatario
Omessa informativa in caso di trattamenti che se male effettuati mettono a rischio libertà fondamentali	162	euro 5.000-30.000	triplicabile in base al reddito del destinatario
Cessione di dati ad esercente non interessato alla salute del paziente	162	euro 500-3.000	—
Comunicazione dei dati da persona non titolata a conoscerli	162	euro 500-3.000	—
Omessa o incompleta notificazione	163	euro 10.000-60.000	pubblicazione ingiunzione di pagamento sui quotidiani
Omessa informazione del Garante od omessa esibizione di documenti richiesti dal Garante	164	euro 4.000-24.000	—

Certo, sarà difficile che questi dati finiscano al giudice a meno che non si dimostri la loro diffusione. Ciò accade:

- quando l'autorità di pubblica sicurezza – intervenuta in seguito a perquisizione o perlustrazione post-effrazione di terzi – o lo stesso paziente denunciino il medico per l'iter scorretto;
- quando si verifica un danno perché qualche "intruso" utilizza i dati sensibili di uno o più pazienti per propri fini.

Nel primo caso, il medico che omette le misure di sicurezza rischierebbe l'ammenda fino a 50 mila euro o due anni di reclusione, ma... niente paura.

Ci sono da due a sei mesi per adeguarsi al momento della denuncia, con notifica entro 60 giorni all'Authority dell'adempimento in corso; a seguito dell'accertamento positivo del Garante, si estinguerà il reato pagando un quarto della pena sopra citata.

Nel secondo caso, c'è un danno di mezzo, che implica un procedimento civile con possibile sentenza che obbliga il medico a un risarcimento ai sensi dell'articolo 2050 del codice civile.

Certo, chi – medico o paziente – avesse utilizzato e diffuso i dati su una malattia o un'attitudine sessuale altrui per creare danni o trarne vantaggi a sé o ad altri rischia di più: fino a tre anni per il dolo specifico (l'intenzione di far male diffondendo il dato), più il

LE SANZIONI PER ILLECITI PENALI

TIPOLOGIA	ARTICOLO	PENA DETENTIVA	PENE DIVERSE-ACCESSORIE
Trattamento di dati personali senza tutela e/o senza previa richiesta di consenso al fine di recare profitti a sé o a terzi o di recare danni ad altri	167	reclusione 6-18 mesi ulteriore pena se c'è danno	eventuale risarcimento danni pubblicazione della sentenza
Diffusione a non aventi titolo di dati personali senza previa richiesta di consenso per recare profitti a sé o terzi o recare danni ad altri	167	reclusione 6-24 mesi ulteriore pena se c'è danno	eventuale risarcimento danni pubblicazione della sentenza
Trattamento di dati sensibili senza titolo o richiesta di consenso al fine di recare profitti o recare danni ad altri	167	reclusione 12-36 mesi ulteriore pena se c'è danno	eventuale risarcimento danni pubblicazione della sentenza
False dichiarazioni o false notificazioni al Garante	168	reclusione 6-36 mesi ulteriore pena se c'è danno	eventuale risarcimento danni pubblicazione della sentenza
Omissione misure di sicurezza	169	reclusione 6-24 mesi se recidivo, riducibile (vedi testo)	in alternativa ammenda da euro 10.000 a 50.000 eventuale risarcimento danni pubblicazione della sentenza
Trattamento in presenza di rigetto dell'autorizzazione o di penenza	170	reclusione 3-24 mesi	eventuale risarcimento danni pubblicazione della sentenza

risarcimento dei danni. Infine, un avviso per chi, ravvisando motivi di gravità tali da dover rendere pubblica una patologia, chiede al Garante l'autorizzazione a divulgare dei dati sensibili e, nel silenzio dell'interlocutore (quindi senza aver ottenuto l'autorizzazione), tratta ugualmente quei dati, rischia fino a due anni di reclusione. In tutti questi casi, inoltre, la sentenza è pubblicata.

Nella tabella sopra sono riportate, articolo per articolo, le san-

zioni penali e amministrative in cui il medico può incappare.

E non va dimenticato che ci sono anche le sanzioni disciplinari (norme del codice deontologico a pagina 4) che comportano il deferimento all'ordine in caso di violazione, il codice penale, che prevede:

- all'articolo 326 (rivelazione di segreto d'ufficio) la reclusione (fino a tre anni, o fino ad un anno se solo colposa) per chi pubblico ufficiale o incaricato di pubblico

servizio rivelasse notizie d'ufficio da tenere segrete o ne agevolasse la conoscenza violando i doveri inerenti al servizio o abusando delle proprie qualità;

- all'articolo 622 (rivelazione di segreto professionale, punibile a querela dell'offeso) la reclusione fino a un anno per chiunque, avendo notizia di un segreto per ragione del proprio stato, ufficio o professione, lo rivela senza giusta causa o lo impiega a proprio o ad altrui profitto.

4.1 - L'evoluzione degli studi medici
Flashback al maggio 2000. Il trattamento dei dati sensibili negli studi dei medici finisce in cronaca nera. Alcune cooperative di medici di medicina generale sono indagate da una Procura del Nord Italia. Si ipotizza che le loro ricerche epidemiologiche siano state svolte senza adeguate garanzie circa la sicurezza dei dati delle schede cliniche degli assistiti di ciascun medico-socio; schede oggetto delle statistiche. Nell'assolvere i medici di famiglia al processo di primo grado, il giudice ha tenuto conto che medicine di gruppo e in rete sempre più hanno bisogno del computer per far dialogare i propri associati, insomma: la tecnologia non corre di pari passo con le norme sulla privacy. E intanto spuntano altri potenziali terreni di conflitto tra norme incentivanti la raccolta di dati sensibili e privacy, come i *trial clinici* sul territorio e la *farmacovigilanza*, che il codice ha inserito quali finalità di rilevante interesse pubblico giustificanti la raccolta dati a fini statistici (artt. 97-100 e 104-110). Al capo III si parla di trattamento di dati a

Il documento programmatico sulla sicurezza, un obbligo che diventa una tutela se si opera offrendo servizi informatizzati

scopi scientifici; tale trattamento è tra quelli che hanno la particolarità di potersi estendere nel tempo illimitatamente (artt. 98-99), anche quando i titolari dei diritti di riservatezza non ci sono più. Dalla lettura (articolo 100) si arguisce che però i dati sensibili, se ricondotti agli interessati, non possono essere diffusi, e che gli stessi interessati possono opporsi qualora derivasse oggettivamente un danno dalla loro diffusione.

4.2 - Trattamento dati per scopi scientifici: trial e farmacovigilanza

Il trattamento dei dati sensibili a fini scientifici entra in gioco se il medico partecipa a progetti di farmacovigilanza o a trial clinici previsti dal decreto 10 maggio 2001. In questi campi tra la teoria delle leggi e la pratica la distanza è considerevole. Partiamo dalla legge.

Per l'articolo 110 del codice (su raccolta dati sensibili a fini di ricerca medica, biomedica ed epidemiologica), non occorre il consenso del cittadino al trattamento dei suoi dati «quando la ricerca è prevista da un'espressa

disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12 bis del dlgs 502/92 (e successive modifiche)» e per il quale sono decorsi 45 giorni dalla comunicazione del trattamento al Garante da parte del titolare, cioè di chi gestisce in modo autonomo la ricerca (l'industria farmaceutica o un istituto scientifico). Il codice aggiunge: «Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante (al titolare, ndr)».

Sperimentazioni cliniche – Per i trial clinici le normative sono mutate dalle *good clinical practices* internazionali, che a loro volta mutuano dalla Carta di Helsinki del 1964 regole stringenti: in base a queste ultime il consenso al trattamento dei dati personali è già inserito nel modello del consenso informato. Dunque, i comitati etici di Asl e ospedali che approvano i protocolli delle aziende, nel fissare le regole per acquisire tale consenso (alla fine firmato dal paziente), di norma stabiliscono gli obblighi pure sul trattamento dei dati

sensibili. Basta un'unica firma nello studio del medico, e il trial va. Ma il medico deve dire al paziente che fine fanno i suoi dati. Chi ha addestrato i primi medici a gestire trial sul territorio (la nostra fonte qui è la Società nazionale di aggiornamento interdisciplinare) sottolinea che qui entrano in gioco tre tipi di documentazione da conservare separatamente: le cartelle cliniche di uso "ordinario"; le cartelle *case report form* dove sono riportate le sole iniziali degli arruolati ed i dati anamnestici con gli esiti degli esami di routine; la documentazione *masterfile* dove sono custoditi tutti i referti cartacei e dove si spiega che quelle iniziali appartengono al signor Tal dei tali. Per quest'ultima è necessaria custodia particolare, mentre i primi due tipi di dati si possono conservare su file. In ogni caso si tratta di tre accessi separati, di cui il medico di famiglia riferirà al paziente. Quest'ultimo secondo il Garante (si veda anche la pronuncia dell' 8 marzo 2000) va edotto in modo chiaro su finalità e durata del trattamento e sul fatto che le informazioni contenute nella cartella clinica saranno utilizzate ed eventualmente comunicate a una o più aziende farmaceutiche indicate nominativamente (articoli 97-98). Va anche dato l'indirizzo della persona o del servizio cui il paziente potrà rivolgersi per esercitare i

diritti di cancellazione, rettifica o aggiornamento dei suoi dati. Il paziente deve sapere, inoltre, se i dati comunicati lo rendono identificabile. Il monitor dell'industria, in genere, ha titolo per accedere ai documenti cartacei per verifiche eventuali (*audit*).

Farmacovigilanza - Anche sul fronte farmacovigilanza, come si rileva dalle esperienze della Società italiana di medicina generale, le *good clinical practices* hanno dato luogo a un sistema di codifica internazionale dei dati dai pazienti. Un medico che rilevasse una reazione avversa in un suo assistito, ne comunica all'Asl solo iniziali, sesso ed età senza citare la data di nascita. L'Asl poi gira i dati al ministero della salute lasciando anonimo pure il nome del medico perché non si risalga al paziente; quel nome al funzionario serve solo in caso di richiesta da parte delle istituzioni di dati aggiuntivi sul caso o nella scheda segnalatrice.

4.3 - Trentun marzo, vola il Dpss
 Siano essi immagazzinati a scopi scientifici o di diagnosi e cura, giacciono in una pila di fogli nell'armadio o al computer, i dati dei pazienti non riposano comunque tranquilli, e il Garante lo sa. Per questo fin dal 2000, anno di applicazione del dpr 318/99, ha chiesto a tutti i medici convenzionati – computerizzati e non – di

redigere il documento programmatico sulla sicurezza (Dpss): un testo lungo (se informatizzato comprendente molti file) che cita le nomine di responsabili e incaricati di trattamento, le misure in caso di distruzione di dati, accesso non autorizzato, trattamento non consentito, manutenzione e inclusivo di allegati e relazioni di esperti. Tale testo va predisposto entro il 31 marzo di ogni anno.

L'incombenza spetta anche ai medici senza personal computer poiché accomuna tutti coloro che gestiscono dati sensibili.

In particolare, si fa dettagliata per i medici che abbiano un collaboratore di quando in quando incaricato di maneggiare le schede dei pazienti. La lista di questi collaboratori va presentata al Garante e aggiornata a ogni novità. Vi vanno delineate le responsabilità di ciascun incaricato, va specificato come avviene l'accesso agli armadi-archivi, quali sono i dispositivi di controllo: chi entra nell'archivio dove i dati vengono conservati dev'essere autorizzato prima e registrato poi!

L'allegato B al Codice (disciplinare tecnico in materia di misure di sicurezza) in realtà specifica con maggiore accuratezza le misure citate dagli articoli 34 e 35 sulla messa in sicurezza dei dati e si rivolge prevalentemente al medico del futuro, che ha il computer e tratta tali dati on-line.

Molti degli accorgimenti qui indicati sono già noti ai medici e scritti nei documenti programmatici sulla sicurezza.

Siti specializzati (www.privacy.it oppure www.cos.it) mettono a disposizione dei fac-simile per facilitare il medico nella compilazione.

4.4 - Disciplinari tecnici di sicurezza

Grazie all'allegato B adesso esiste in pratica un vademecum per compilare il Dpss. Il codice ora prescrive che il medico di famiglia e il pediatra di libera scelta

spiegheranno entro il 31 marzo di ogni anno:

- che tipo di dati vengono trattati nei loro studi;
- chi li tratta, con quali compiti e in quale qualità (titolare, responsabile, incaricato);
- quali rischi incombono sui dati e gli accorgimenti presi per impedirne il danneggiamento;
- quale tipo di formazione viene fatta agli incaricati;
- quali criteri vanno adottati se si affidano i dati all'esterno (anche all'azienda sanitaria locale?);
- come viene separata la gestione dei dati sensibili da quella de-

ADEMPIMENTI E SCADENZE SUB ALLEGATO B

Ogni settimana	Attivare la procedura di salvataggio dei dati sensibili e personali dei pazienti
Ogni tre mesi	Modificare la password
Ogni sei mesi	Attivare gli strumenti di protezione dei dati degli assistiti Aggiornare i programmi antivirus
Ogni anno	Verificare le funzioni attribuite agli incaricati Compilare ed inviare al Garante il documento programmatico sulla sicurezza
Secondo avvenimenti	Disattivare la password non utilizzata da sei mesi Aggiornare il documento programmatico sulla sicurezza

gli altri dati personali. Nel disciplinare si trovano regole semplici («lo strumento elettronico non va lasciato accessibile durante le sessioni di trattamento») e altre più complesse: come si conservano i floppy disk con i file delle cartelle dei pazienti, come si separano i dati acquisiti nella diagnosi e cura da quelli acquisiti a fini scientifici, e da quelli raccolti per ricerche genetiche, dalle ricette per i tossicodipendenti e da quelli dei malati Hiv.

Agli installatori vanno chieste minuziose descrizioni scritte dell'intervento effettivo, da allegare. Il disciplinare quindi spiega compiti e responsabilità dei collaboratori.

L'incaricato del trattamento dei dati sensibili con strumenti elettronici (medico-socio, infermiere, collaboratore di studio) va dotato di una personale credenziale di autenticazione che può esprimersi nelle tre seguenti modalità alternative:

- 1 – Codice personale e non cedibile per l'identificazione dell'incaricato + password riservata di otto caratteri da modificare ogni tre mesi, nota a lui solo, non agevolmente riconducibile a lui;
- 2 – Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato + codice personale e non cedibile

per l'identificazione e/o password riservata di otto caratteri da modificare ogni tre mesi;

- 3 – Impronta digitale od altra caratteristica biometrica dell'incaricato + codice personale e non cedibile per l'identificazione e/o password riservata di otto caratteri da modificare ogni tre mesi.

La credenziale va tenuta segreta con appositi sistemi da citare nel documento. Va disattivata se non è usata da sei mesi o se l'incaricato cambia posto di lavoro. Il titolare dà disposizione scritta di come, in sua assenza, possano essere resi disponibili i dati trattati a chi, titolato, li richieda. Se gli incaricati a trattare i dati lo sono in relazione a mansioni differenti, occorre articolare un sistema di autorizzazioni stabilendo prima dell'inizio di ogni trattamento chiare regole scritte da inserire nel documento programmatico.

Le condizioni dei profili autorizzativi attribuiti vanno verificate ogni anno. Altre scadenze: i dati degli assistiti sono protetti dagli hackers attivando idonei strumenti elettronici da aggiornare almeno ogni sei mesi. Con la stessa cadenza vanno aggiornati i programmi antivirus.

I dati vanno salvati con procedura settimanale.

UN'IPOTESI DI MODELLO DI CONSENSO

Il sottoscritto nato a
ile residente
a.....

assistito dal Dott..... e dallo stesso informato sui diritti e sui limiti di cui alla Legge n. 675/96 concernente "la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" autorizza il Dott..... ed in sua assenza i medici sostituiti associati, nonché il personale collaboratore dei suddetti sanitari a raccogliere, registrare ed utilizzare i dati personali ai fini di diagnosi e cura, a fini sanitari, a fini amministrativi e fiscali.

Inoltre il sottoscritto acconsente a che sia data comunicazione relativa al proprio stato di salute alle persone qui indicate:

- 1).....
- 2).....

Il sottoscritto infine acconsente a che il ritiro della propria documentazione sanitaria (ivi comprese ricette mediche, richieste specialistiche, referti di indagini, cartelle cliniche) venga effettuato dalle seguenti persone:

- 1).....
- 2).....

E' a conoscenza del fatto che i dati raccolti e detenuti in base ad obblighi di legge non necessitano di consenso al trattamento.

Firma dell'interessato o dell'esercitante la patria potestà

Tra i possibili fac-simili studiati con il Garante per la raccolta del consenso al trattamento dei dati nello studio del generalista proponiamo questo pubblicato a settembre 2002 sul sito del Bollettino dell'Ordine dei medici di Modena, da sempre tra i più attenti alla tematica.

Fonte: Bollettino Ordine dei medici di Modena settembre 2002

GLI ARTICOLI DEL CODICE CITATI SU QUESTO VOLUME

PARTE I – DISPOSIZIONI GENERALI (TITOLI I-VII)

Art. 4 - Trattamento dei dati pag. 12

Regole per tutti i trattamenti (Titolo III – Capo I)

Art. 9 – Modalità di esercizio dei diritti dell'interessato pag. 9

Art. 10 - Riscontro all'interessato pag. 9

Art. 11 – Modalità del trattamento e requisiti dei dati pag. 9

Art. 12 - Codici di deontologia e buona condotta pag. 19

Art. 13 – Informativa pag. 15

Regole ulteriori per i soggetti pubblici (Titolo III – Capo II)

Art. 18 – Principi applicabili a tutti i trattamenti effettuati dai soggetti pubblici pag. 19

Art. 19 – Principi per il trattamento di dati diversi dai sensibili o giudiziari pag. 19

Art. 20 – Principi applicabili al trattamento di dati sensibili pag. 19

Art. 21 – Principi applicabili al trattamento di dati giudiziari pag. 19

Art. 22 – Principi applicabili al trattamento di dati sensibili e giudiziari pag. 19

Art. 24 - Dati che possono essere trattati senza consenso pag. 12

Soggetti che effettuano il trattamento (Titolo IV- Capo I)

Art. 28 – Titolare del trattamento pag. 19

Art. 29 – Responsabile del trattamento pag. 19

Art. 30 – Incaricato del trattamento pag. 20

Misure minime di sicurezza (Titolo IV – Capo II)

Art. 34 – Trattamenti con strumenti elettronici pag. 28

Art. 35 – Trattamenti senza l'ausilio di strumenti elettronici pag. 20

Art. 36 – Adeguamento pag. 21

Adempimenti (Titolo V)

Art. 39 – Obblighi di comunicazione al Garante (notificazione) pag. 13

Trasferimento di dati all'estero (Titolo VII)

Art. 42 – Trasferimenti di dati all'interno dell'Unione Europea pag. 22

Art. 43 – Trasferimenti consentiti in paesi terzi pag. 22

Art. 44 – Altri trasferimenti consentiti pag. 22

Art. 45 – Trasferimenti vietati pag. 22

TRATTAMENTI DI DATI PERSONALI IN AMBITO SANITARIO (PARTE II – DISPOSIZIONI RELATIVE A SPECIFICI SETTORI - TITOLO IV - CAPI II-VI)

Modalità semplificate di informativa e consenso (Capo II)

Art. 78 – Informativa del medico di medicina generale o del pediatra pagg. 15-16

Art. 79 – Informativa da parte di organismi sanitari pag. 16

Art. 80 – Informativa da parte di altri soggetti pubblici pag. 16

Art. 82 – Emergenze e tutela della salute e dell'incolumità fisica pag. 17

Art. 83 – Altre misure per il rispetto dei diritti degli interessati pagg. 14-15-21

Art. 84 - Comunicazione di dati all'interessato pag. 14

Finalità di rilevante interesse pubblico (Capo III)

Art. 85 – Compiti del Servizio sanitario nazionale pag. 13

Art. 86 – Altre finalità di rilevante interesse pubblico pag. 13

Prescrizioni mediche (Capo IV)

Art. 87 – Medicinali a carico del Servizio sanitario nazionale pagg. 17-18

Art. 88 – Medicinali non a carico del Servizio sanitario nazionale pag. 18

Art. 89 – Casi particolari pag. 18

I n d i c e r a g i o n a t o

Dati genetici (Capo V)

Art. 90 – Trattamento dei dati genetici e donatori di midollo osseo pag. 18

Disposizioni varie (Capo VI)

Art. 92 – Cartelle cliniche pag. 21

Art. 93 – Certificato di assistenza al parto pag. 21

Trattamento di dati a scopi scientifici (Parte II – Titolo VII)

Art. 97 – Ambito applicativo pag. 27

Art. 98 – Finalità di rilevante interesse pubblico pag. 27

Art. 99 – Compatibilità tra scopi e durata del trattamento pag. 27

Art. 110 - Ricerca medica, biomedica ed epidemiologica pag. 26

PARTE III – TUTELA DELL'INTERESSATO E SANZIONI

Sanzioni (Parte III – Titolo III)

Art. 161 – Omessa o inadeguata informativa all'interessato pag. 23

Art. 162 – Altre fattispecie pag. 23

Art. 163 – Omessa o incompleta notificazione pag. 23

Art. 164 – Omessa informazione o esibizione al Garante pag. 23

Art. 167 – Trattamento illecito di dati pag. 25

Art. 168 – Falsità nelle dichiarazioni e notificazioni al Garante pag. 25

Art. 169 – Misure di sicurezza pag. 25

Art. 170 – Altre fattispecie pag. 25

Norme finali (Parte III - Titolo IV – Capo IV)

Art. 186 – Entrata in vigore pag. 6