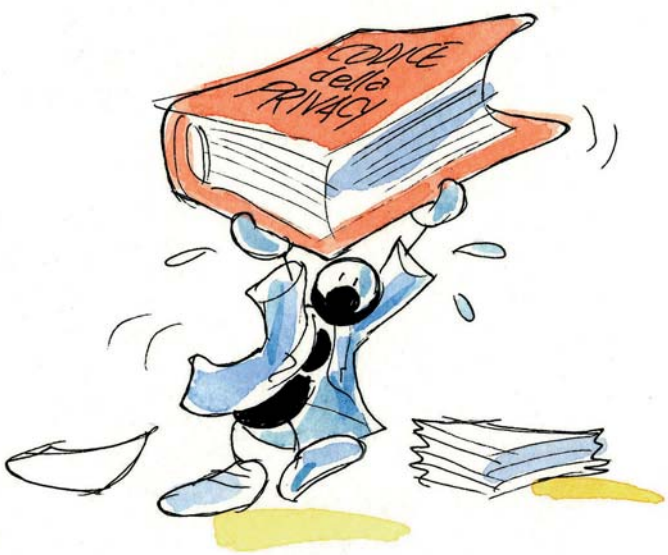
SOCIETÀ ITALIANA DI RADIOLOGIA MEDICA

Documenti SIRM 2005

Il Codice della Privacy: istruzioni per l'uso



Maurizio Centonze
Adriano Fileni
Francesco Dalla Palma

Supplemento de "Il Radiologo" 3/2005

Il Codice della Privacy: istruzioni per l'uso
www.sirm.org - Documenti SIRM
Aggiornamento e professione

Settembre 2005

OMICRON Editrice Genova - *omicred@tin.it - www.omicred.com*

Introduzione

In seguito all'introduzione della legge 675/96, le successive integrazioni ed il recente decreto legislativo 196/03, il cosiddetto Codice della Privacy, la tutela del diritto alla riservatezza dei dati personali e sensibili del Paziente/Utente è diventata parte integrante della professione medica. Nel contesto sanitario e, soprattutto, nei Servizi e Studi radiologici, che effettuano oltre 45 milioni di esami all'anno, l'attuazione della normativa pone problematiche maggiori rispetto ad altri settori.

Conseguentemente anche il Radiologo ha dovuto adottare una serie di processi lavorativi ed organizzativo-gestionali, per molti aspetti differenti dai consueti comportamenti ed atteggiamenti professionali. Tutto ciò è stato recepito da molti come ulteriore aggravio burocratico mentre pochi hanno colto il senso innovativo e la significativa svolta della normativa.

Uno dei compiti del Radiologo del nuovo millennio consiste nell'interpretare le nuove disposizioni in materia di privacy non già come ulteriore imposizione amministrativa, bensì, cogliendone il significato originario (difesa dei diritti, delle libertà fondamentali e della dignità della persona), come un'occasione d'innovazione, processo continuo - culturale ed organizzativo - di sviluppo del rapporto Struttura/Utente e irrinunciabile opportunità di miglioramento della qualità.

In tale ottica l'applicazione della legge non deve più essere passiva e sterile ma tradursi in una vera e propria "cultura del rispetto", finalizzata a garantire – nei modi e nella sostanza – la sfera di riservatezza, diritto del Paziente/Utente.

Questo documento non ha la pretesa di sostituirsi al Codice della Privacy, che ogni singolo lavoratore e professionista dell'ambito sanitario è tenuto a leggere, ma intende rappresentare una guida, una sorta di viatico per addentrarsi in un argomento solo apparentemente lontano dalla realtà operativa del Radiologo. Il documento è strutturato in una serie di domande le cui risposte si propongono di offrire, se non una descrizione esaustiva della vera e propria rivoluzione introdotta da questa legge, almeno dettagliati rimandi alle principali definizioni ed adempimenti ai quali si deve provvedere per non incorrere nelle sanzioni - a volte anche molto pesanti - previste dalla normativa.

Che cosa è la Privacy?

È un termine inglese che è entrato nell'uso comune, traducibile con "riservatezza", da non confondere con il diritto al segreto.

Il diritto alla privacy nasce nei paesi anglosassoni verso la fine del 1800 e si configura con il *"diritto di essere lasciato in pace"*, cioè di non subire intrusioni indesiderate nella sfera della propria vita privata.

Nella società in cui viviamo, la velocità e la facilità di raccolta, interconnessione ed elaborazione dei dati, associate all'incremento del valore economico e strategico delle informazioni, non solo nel contesto economico, hanno determinato un'evoluzione del concetto di privacy che attualmente contempla anche il "*diritto al controllo dei propri dati personali* " attraverso un insieme di regole di comportamento rivolte a tutti coloro che effettuano operazioni sui medesimi.

Quali sono le norme che regolamentano la Privacy?

Il decreto legislativo 196 del 30 giugno 2003, ovvero il Codice della Privacy, rappresenta il testo unico volto ad assicurare che il trattamento dei dati personali si svolga nel pieno rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'Interessato.

Nella genesi dell'attuale normativa vanno ricordate due tappe fondamentali: la direttiva 95/46/CE del Parlamento e del Consiglio d'Europa, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione dei dati; la legge n. 675 del 31 dicembre 1996.

Quali finalità si propone il Codice della Privacy?

Il Codice della Privacy garantisce che "*…il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'Interessato…*" (Art. 2, comma 1). A quest'ultimo proposito, la norma fa particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Cosa è il trattamento dei dati?

Si considera tale qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di strumenti elettronici o comunque automatizzati, che consentano la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati personali a prescindere dalla presenza delle informazioni in una banca dati (Art. 4, comma 1, lettera a).

Quest'ultima precisazione scongiura eventuali dubbi sulla applicabilità della norma anche alle informazioni non strutturate in un archivio cartaceo o informatico.

È intuitivo il fatto che la normativa abbia una sorta di "immanenza giuridica" in qualunque attività lavorativa – svolta con materiale cartaceo o con mezzi elettronico-informatici - che preveda l'utilizzo di dati personali.

Tra le attività ricomprese nella sfera del trattamento, comunicazione e diffusione meritano qualche precisazione al fine di evitare fraintendimenti:

per *comunicazione* si intende il dare conoscenza, in qualunque forma, dei dati a uno o più soggetti determinati che siano diversi dall'Interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati. La *diffusione* rappresenta, invece, il dare conoscenza dei dati a soggetti indeterminati (es. pubblicazione di una banca dati su Internet) e può avvenire anch'essa in qualunque forma, ivi compresa la loro messa a disposizione o consultazione.

Quali sono i dati personali?

Il Codice della Privacy nell'Art. 4, comma 1, lettere da b) ad e) individua quattro distinte tipologie di dati:

1. *Dato personale*: qualunque informazione relativa sia a persone fisiche che giuridiche, identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (es. il codice fiscale).

2. *Dato identificativo*: qualunque informazione che consenta un'identificazione diretta dell'Interessato (es. dato anagrafico).
3. *Dato sensibile*: qualunque informazione idonea a rivelare l'origine razziale ed etnica, le opinioni politiche, filosofiche e religiose, le **condizioni di salute** (dati sanitari), l'adesione a partiti, sindacati o altre organizzazioni e le abitudini sessuali. Per tali dati la normativa assicura garanzie maggiori rispetto ad altre categorie, in considerazione dei maggiori rischi che possono derivare all'Interessato dalla loro circolazione.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono comunemente considerati i più delicati tra i dati sensibili poiché sono potenzialmente in grado di mettere a nudo l'individuo, evidenziandone le eventuali debolezze ed esponendolo maggiormente al concreto pericolo di discriminazioni sociali.

4. *Dato giudiziario*: qualunque informazione idonea a rivelare eventuali provvedimenti di cui all'Art. 3, comma 1 lettere da a) ad o) e da r) ad u) del D.P.R. 14 novembre 2002 n. 313 e la qualità di imputato o, comunque, di indagato ai sensi degli Artt. 60 e 61 del codice di procedura penale.

Categoria opposta al dato personale è quella del *dato anonimo*, che comprende quelle informazioni che, in origine o in seguito a trattamento, non sono associabili ad un Interessato identificato o identificabile (Art. 4, comma 1, lettera n). Come stabilito dal Garante, non possono essere considerati tali quei dati che, pur non consentendo direttamente la identificazione dell'Interessato, se associati ad altre informazioni permettano comunque di risalire a quest'ultimo (es. dati criptati).

Ricorda: la legge prevede maggiori garanzie per i dati sensibili come quelli sanitari

Chi sono i soggetti protagonisti del trattamento dei dati?

Facendo riferimento al trattamento dei dati, il Codice della Privacy individua due distinte categorie di soggetti:

1. *Passivi*: l'**Interessato**, cioè colui (persona fisica o giuridica, ente o associazione) al quale si riferiscono i dati personali (Art. 4, comma 1, lettera i).
2. *Attivi*: tutti coloro che eseguono le attività ricomprese nel trattamento medesimo.

Ai sensi dell'Art. 4, comma 1, lettera f) il Codice identifica nel **Titolare** del trattamento la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro Titolare le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali, nonché agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Rispetto alla definizione contenuta nella precedente normativa (675/96) il Codice ha dato rilievo alla figura della contitolarità, che nell'ambito sanitario richiama a due differenti soggetti: l'azienda sanitaria pubblica o la struttura privata e il Medico di Medicina Generale.

Come precisato dal Garante (comunicato stampa del 11 dicembre 1997 nel n. 2 del Bollettino del Garante, p. 75), nell'ambito di un'amministrazione pubblica quale un'azienda sanitaria va considerato Titolare l'entità nel suo complesso (Art. 28) e non già le singole persone fisiche che amministrano o rappresentano la struttura, anche se quest'ultima opererà, nelle decisioni che di volta in volta verranno assunte, proprio per il tramite di tali soggetti.

Non è mancato peraltro chi, all'indomani dell'entrata in vigore già della legge 675/96, ha sottolineato la necessità della individuazione di una persona fisica Titolare, motivandola da un lato con la similitudine tra legge della privacy e assetto normativo in tema di sicurezza dei posti di lavoro, dall'altro con il fatto che il Codice è corredato da un forte apparato sanzionatorio, anche di natura penale. Peraltro lo stesso Garante in risposta al Ministero delle Finanze e alle Ferrovie dello Stato che avevano sottosposto al suo parere tale questione scrive *"...se la singola direzione generale o area eser-*

cita, tramite i propri organi, un potere decisionale reale del tutto autonomo sulle finalità e sulle modalità dei trattamenti effettuati nel proprio ambito, non condizionato da scelte effettuate a livello centrale o di vertice, la medesima direzione o area potrebbe essere considerata come Titolare dei trattamenti (ovvero anche come contitolare del trattamento, a seconda dei casi)". Pertanto, anche in considerazione del d.lgs. 229/99 (riforma Bindi), il Titolare del trattamento dei dati in un'azienda sanitaria pubblica deve essere considerato il Direttore Generale, in quanto colui che adotta l'atto aziendale di organizzazione e funzionamento di diritto privato, responsabile della gestione complessiva e della nomina dei direttori delle strutture operative dell'azienda. Nel caso di cliniche o di organismi sanitari privati la rappresentanza del Titolare dovrà essere individuata in base alle disposizioni statutarie in capo agli organi deputati a manifestare la volontà all'esterno o ad assumere atti di impegno (es. presidente del consiglio di amministrazione, amministratore delegato…). Per i soggetti accreditati o convenzionati con il SSN che non godono di autonomia ma che agiscono in nome e per conto di un'azienda sanitaria si profila la opportunità di procedere alla nomina degli stessi come Responsabili del trattamento (vedi paragrafo successivo). Se invece ci si riferisce agli studi medici privati, ivi compresi quelli radiologici, i singoli o le associazioni di professionisti dovranno essere considerati Titolari.

Un'ulteriore figura prevista dal Codice della Privacy è quella del **Responsabile**, ovvero la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposto dal Titolare al trattamento dei dati personali (Art. 4, comma 1, lettera g). Al Responsabile, la cui nomina da parte del Titolare è facoltativa (Art. 29, comma 1), compete di assicurare il costante rispetto della normativa da parte del personale dell'impresa, ente o amministrazione.

La eventuale nomina, che nel caso sia necessario per esigenze organizzative può essere plurima con suddivisione dei compiti e delle mansioni (comma 3), deve necessariamente ricadere tra soggetti che per esperienza, capacità ed affidabilità forniscano adeguate garanzie del pieno rispetto delle disposizioni in materia di trattamento non ultimo il profilo relativo alla sicurezza, stante la delicatezza del mandato, particolarmente ampio (comma 2).

Il legislatore delegato ha pertanto voluto individuare, nell'ambito dell'attività di gestione dei trattamenti, specifici centri di autonomia ma anche di eventuale imputazione di responsabilità. Il Responsabile, che deve ricevere i compiti affidatigli analiticamente specificati per iscritto (comma 4), si attiene alle istruzioni impartite dal Titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e delle proprie istruzioni (comma 5).

Nello specifico ambito radiologico il Responsabile potrebbe corrispondere con il Direttore di Dipartimento o di Struttura Complessa. Poiché la nomina può essere affidata anche ad un soggetto non dipendente direttamente dal Titolare, di cui quest'ultimo si avvalga per lo svolgimento di specifiche attività (es. contratti e programmi di manutenzione), le ditte produttrici di apparecchiature, di pellicole o comunque qualsiasi fornitore di beni o servizi per imaging diagnostico può configurarsi come Responsabile: ciò consente di evitare la rigida disciplina prevista per la comunicazione di dati personali, che si integrerebbe nel caso in cui il soggetto esterno non fosse nominato Responsabile.

Il terzo ed ultimo soggetto attivo del trattamento dei dati è rappresentato dall'**Incaricato**, persona fisica autorizzata dal Titolare o, laddove designato, dal Responsabile a compiere operazioni di trattamento (Art. 4, comma 1, lettera h).

Il primo comma dell'Art. 30 ribadisce con forza che le operazioni di trattamento possono essere effettuate solo da Incaricati che operano sotto la diretta autorità del Titolare o del Responsabile e che si attengono rigorosamente alle istruzioni impartite.

Come per i Responsabili, anche la designazione degli Incaricati viene effettuata per iscritto in un documento protocollato in cui sono individuati puntualmente l'ambito o gli ambiti del trattamento consentiti.

Si considera tale anche la documentata preposizione della persona fisica ad una unità operativa per la quale è individuato per iscritto l'ambito del trattamento consentito agli addetti all'unità medesima: si legalizza pertanto una diffusa prassi applicativa (circolari aziendali o amministrative di nomine effettuate per categorie di dipendenti appartenenti al medesimo settore, qualora l'ambito di trattamento dagli stessi eseguito sia il medesimo), introducendo un'indubbia forma di semplificazione per i Titolari e i Responsabili, senza peraltro inficiare il significato stesso della nomina.

La forma scritta della nomina ad Incaricato o Responsabile risponde da un lato all'esigenza di individuare un mezzo attraverso il quale siano fornite indicazioni precise al soggetto attivo del trattamento dati e dall'altro di dare certezza dell'adempimento da parte del Titolare o del Responsabile.

Ricorda: il Responsabile e l'Incaricato devono essere nominati per iscritto

Chi garantisce la corretta applicazione della normativa?

Il **Garante**, che appartiene al novero delle autorità amministrative indipendenti, ha il compito di sorvegliare l'applicazione delle disposizioni del Codice della Privacy. Il Garante, organo che opera in piena autonomia ed indipendenza di giudizio e valutazione, è costituito da quattro componenti (due eletti dalla Camera dei Deputati e due dal Senato della Repubblica) che rimangono in carica quattro anni con possibilità di un'unica riconferma.

Quali sono gli obblighi relativi al trattamento?

Ogni Titolare, sia pubblico che privato, deve rispettare precise modalità di raccolta e di elaborazione dei dati personali come stabilito dall'Art. 11 del Codice della Privacy. In particolare, i dati oggetto di trattamento devono essere: trattati in modo lecito e corretto; raccolti e registrati per scopi determinati, espliciti e legittimi; esatti e aggiornati; pertinenti, completi e non eccedenti rispetto alla finalità del trattamento; conservati per un periodo di tempo non superiore a quello strettamente necessario alle finalità del trattamento.

A proposito del diritto all'oblio dell'Interessato, ovvero al diritto di essere dimenticato, il Codice

della Privacy sembra entrare in contrasto con la normativa vigente a riguardo della conservazione ed archiviazione della documentazione radiologica e dei relativi referti, sia in forma cartacea che elettronica (rispettivamente 10 anni e illimitata). Tale contrasto è tuttavia solo apparente, stante la prevalenza della norma precedente, intesa a tutelare i diritti di salute dell'Interessato (Costituzione italiana Art. 97, D.P.R. 27 marzo 1969 numero 128 Artt. 2-5, 7, D.P.R. 14 marzo 1974 numero 225, nuovo codice di deontologia medica Art. 10, Circolare Ministero della sanità 19 dicembre 1986).

Ricorda: i dati raccolti devono essere completi ma non eccedenti le finalità alle quali si riferiscono

Quali informazioni devono essere fornite all'Interessato?

Il Codice della Privacy dedica l'Art. 13 alla disciplina generale dell'informativa, necessaria per la raccolta del consenso al trattamento dei dati. L'Interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa le finalità e modalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto, i soggetti ai quali i dati possono essere comunicati, gli ambiti di diffusione dei medesimi, i diritti ed, infine, gli estremi identificativi del/i Titolare/i e dell'eventuale/i Responsabile/i e più specificamente, qualora designato, quello deputato per il riscontro dei diritti dell'Interessato.

Nell'ambito sanitario (Art. 77 del Titolo V del Codice della Privacy) la consapevolezza della complessità delle disposizioni di legge porta ad individuare modalità semplificate per l'informativa ed il successivo consenso, in grado di coniugare le necessità amministrative connesse alle prestazioni sanitarie con i diritti del cittadino. Tale semplificazione è applicabile da tre categorie di soggetti:

1. gli organismi sanitari pubblici;
2. gli organismi sanitari privati e gli esercenti le professioni sanitarie;
3. servizi di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.

Come stabilisce l'Art. 78, il Medico di Medicina Generale o il Pediatra di libera scelta informano l'Interessato relativamente al trattamento dei dati personali in forma chiara e tale da rendere facilmente comprensibili gli elementi previsti dall'Art. 13.

L'elemento innovativo rispetto alla precedente normativa consiste nel fatto che l'informativa è valida per il complessivo trattamento dei dati necessario per l'attività sanitaria svolta dal medico, nonché per ogni trattamento correlato, effettuato dal collega che sostituisce temporaneamente il medico o il pediatra, da chi fornisce la prestazione specialistica richiesta, da chi può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata e da chi fornisce i farmaci prescritti.

L'informativa è di regola fornita per iscritto, anche attraverso specifica documentazione e deve contenere, non solo gli elementi previsti dalla legge, ma anche elementi aggiuntivi collegati ad eventuali trattamenti di dati che avvengano per scopi scientifici, nell'ambito di attività di tele-assistenza e tele-medicina (tele-radiologia!) o comunque di servizi offerti attraverso reti di comunicazione elettronica (Internet, Intranet).

L'articolo successivo (Art. 79) riguarda l'informativa da parte di organismi sanitari pubblici e privati che si avvalgono delle medesime modalità semplificate; una volta fornita, l'informativa vale per la pluralità di prestazioni erogate anche da distinti reparti e

unità dello stesso organismo o di più strutture ospedaliere e territoriali specificamente identificate. È importante che l'organismo o le strutture annotino l'avvenuta informativa con modalità uniformi e con adeguate misure organizzative per consentirne successivamente la verifica anche da parte di altri reparti, nonché l'utilizzo per più trattamenti.

Anche i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti effettuati. Cartelli idonei ed avvisi visibili al pubblico devono integrare l'informativa fornita dagli organismi sanitari, facendo meglio conoscere le finalità della legge sulla privacy e, soprattutto, i diritti del cittadino.

Ricorda: in ambito sanitario l'informativa per il trattamento dei dati personali deve essere fornita preferibilmente per iscritto ma sono previste modalità semplificate

È necessario il consenso dell'Interessato per il trattamento dei dati?

Nel contesto generale, per i soggetti privati e gli enti pubblici economici il trattamento dei dati personali è consentito solo previo consenso informato espresso dall'Interessato. *Nel caso di dati sensibili tale consenso deve essere prestato esclusivamente in forma scritta.*

Per gli enti pubblici non economici il trattamento dei dati personali e sensibili è consentito solo per lo svolgimento delle funzioni istituzionali. Non è necessario acquisire il consenso dell'Interessato, salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici per i quali è assolutamente obbligatorio e può essere manifestato con un'unica dichiarazione sia per iscritto che oralmente. In quest'ultima eventualità, il consenso deve essere comunque documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico da cui risulti anche la fase informativa resa precedentemente all'Interessato. Qualora il Medico di Medicina Generale o il Pediatra forniscano l'informativa per conto di altri professionisti, devono essere adottate idonee modalità per rendere conoscibile anche il consenso.

L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione:

1. per emergenza sanitaria o di igiene pubblica;
2. nel caso di impossibilità fisica, incapacità d'agire o di intendere e volere dell'Interessato, quando non sia possibile acquisire il consenso di chi esercita legalmente la potestà, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'Interessato;

3. nel caso di rischio grave, imminente o irreparabile per la salute o l'incolumità fisica dell'Interessato;
4. in caso di prestazione medica, che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

Ricorda: per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici l'acquisizione del consenso informato al trattamento dei dati sensibili è obbligatoria

Quali misure organizzative per la tutela dei diritti e della dignità dell'Interessato sono previste dal Codice della Privacy?

Il Codice introduce alcune misure organizzative al fine di innalzare il livello di tutela dei diritti e della dignità dell'Interessato.

Nello specifico, l'Art. 83 stabilisce che gli organismi sanitari pubblici e privati, oltre alle misure previste dalle norme in materia di modalità di trattamento dei dati sensibili, adottino:

a) soluzioni che permettano di rispettare un ordine di precedenza e chiamata degli Interessati prescindendo dalla loro individuazione nominativa (ad esempio tramite numeri);

Il problema sembra apparentemente di difficile soluzione per le Unità Operative di Radiologia con molte diagnostiche, poiché ciò costringerebbe ad un'ulteriore regolamentazione degli accessi alle varie sale, al fine di evitare spiacevoli, oltre che potenzialmente dannosi, errori (ad esempio numeri di colore differente per ogni sala diagnostica). Come si può immaginare tutto ciò, oltre a risultare poco gradito ai Pazienti (secondo il sondaggio FIMMG del 26 gennaio 2004, l'86% di essi rifiuta la chiamata per numero) introduce un ulteriore aggravio burocratico all'attività lavorativa quotidiana già estremamente condizionata - per non dire soffocata - da compiti amministrativi dipendenti dalla dinamica legislativa ed organizzativa del nostro sistema sanitario. Nella lettera del 6 febbraio 2004 indirizzata al Ministro della Sanità, il presidente dell'Autorità Garante per la protezione dei dati personali scrive testualmente *"Possiamo fin d'ora anticiparLe che le misure da adottare per tutelare le persone* [Interessati, ndr] *nelle situazioni di promiscuità o in occasione di prestazioni sanitarie, in attuazione dell'Art. 83 del Codice, interesseranno solo le strutture sanitarie e non le anticamere dei singoli medici di base, i quali hanno un rapporto diverso e più personalizzato con i propri assistiti*". Pertanto, se il problema viene risolto per i Medici di Medicina Generale, rimane in tutta la sua complessità per tutti gli altri esercenti le professioni sanitarie, ivi compreso il Radiologo. Tuttavia, la norma si limita ad individuare le finalità di tutela piuttosto che le precise modalità attraverso cui perseguire lo scopo in questione: con ciò si demanda ai soggetti cui la norma si rivolge la scelta discrezionale circa gli strumenti da adottare in ogni singolo caso, per ottemperare nel modo migliore al dettato legislativo, compatibilmente con le peculiarità organizzative del servizio o la natura delle prestazioni che devono essere erogate. La soluzione di prevedere l'individuazione numerica anziché nominativa degli Interessati, nonostante venga utilmente applicata in altre situazioni (ad esempio Ambulatori di Analisi Chimico-Cliniche), non risulta affatto appropriata per i Servizi di Radiologia, quantomeno per quelli di maggiori dimensioni e complessità organizzativa dotati di molteplici sale diagnostiche, cui i Pazienti possono essere destinati. In siffatto contesto appare evidente la sproporzione tra l'ipotetico pregiudizio alla riservatezza dell'Interessato che si intende tutelare ed il rischio potenziale per la sua salute in conseguenza di un'errata identificazione, indotta da un sistema di chiamata basata su un codice numerico. Ancora più in dettaglio, il Codice Deontologico e la normativa sulla radioprotezione non ammettono, per ovvi motivi, errore alcuno nella individuazione della persona alla quale vengono erogate radiazioni ionizzanti o somministrati medicinali o mezzi di contrasto indispensabili per la diagnostica per immagini.

b) appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere (ad esempio righe di delimitazione sul pavimento o cartelli in prossimità degli sportelli);

c) soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute (ad esempio locali dedicati alla raccolta dell'anamnesi);

d) cautele volte ad evitare che le prestazioni sanitarie avvengano in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti (ad esempio uso di paraventi o pareti mobili);

e) il rispetto della dignità dell'Interessato in occasione della prestazione medica e in ogni operazione di trattamento di dati;

f) opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma, anche telefonica, ai soli terzi legittimati di una prestazione di pronto soccorso;

g) adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli Interessati nell'ambito dei reparti, informandone preventivamente gli Interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà.

Si rammenta che la "Carta dei servizi pubblici sanitari" prevede come eccezione che il degente possa richiedere che la sua presenza non sia resa nota;

h) procedure e momenti di formazione del personale diretti a prevenire nei confronti di estranei un'esplicita correlazione tra l'Interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;

i) la sottoposizione degli Incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe a quest'ultimo.

Ricorda: compatibilmente con i vincoli logistici ed organizzativi, adotta tutte le misure atte a tutelare la dignità e i diritti del Paziente

Quali sono le garanzie di sicurezza dei dati previsti dal Codice?

Qualunque dato deve essere custodito in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità di raccolta. A tale scopo devono essere predisposte tutte le idonee misure di sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Eventuali danni subiti dagli Interessati dovranno ottenere risarcimento.

La protezione dei dati personali attraverso adeguate misure di sicurezza ricorre in più parti del Codice: nell'Art. 4 vengono elencate le definizioni con l'obiettivo di evitare o quantomeno ridurre eventuali equivoci interpretativi; il Titolo V è invece una parte completamente dedicata alla sicurezza dei dati e dei sistemi in cui vengono prescritti gli obblighi di sicurezza, i particolari Titolari, le misure minime per i trattamenti svolti con l'ausilio di strumenti elettronici o informatici e l'obbligo di aggiornamento di tali misure; infine, nel Disciplinare Tecnico (Allegato B del Codice) sono specificate le modalità tecniche da adottare per le misure minime di sicurezza a cura del Titolare, del Responsabile e dell'Incaricato.

Secondo quanto previsto dall'Art. 33 i Titolari e, laddove designati, i Responsabili sono tenuti ad adottare misure minime di sicurezza volte ad assicurare un livello minimo di protezione dei dati.

Le misure minime sono elencate nei due articoli successivi e sono distinte per i trattamenti effettuati con (Art. 34) o senza (Art. 35) l'utilizzo di strumenti elettronici. Il trattamento dei dati tramite elaboratori centrali, reti telematiche o, più comunemente, personal computer è consentito solo qualora si adottino sistemi di autenticazione informatica, di gestione delle credenziali di autenticazione (codice identificativo, parola chiave, caratteristica biometrica), di autorizzazione, di aggiornamento periodico dell'ambito del trattamento, di protezione degli strumenti elettronici, di custodia di copie di sicurezza e ripristino dati.

Il Titolare dovrà inoltre redigere e mantenere aggiornato un documento programmatico sulla sicurezza (DPS).

Vi è un "quid pluris" per gli organismi sanitari che consiste nella adozione di tecniche di crittografia per i dati sensibili.

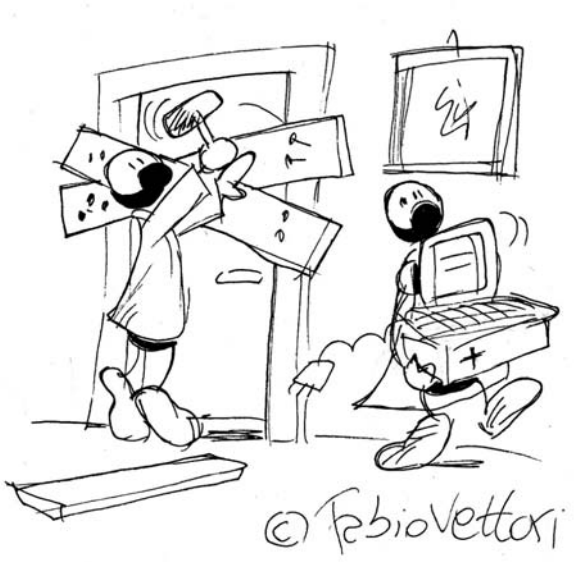
Per il trattamento dei dati senza l'ausilio di strumenti elettronici oltre all'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e alle unità organizzative, si dovranno adottare procedure di custodia degli incartamenti affidati agli stessi per lo svolgimento dei relativi compiti nonché di conservazione di determinati atti in archivi ad accesso selezionato.

Nel Disciplinare Tecnico vengono esplicitate le modalità tecniche da adottare da chiunque effettui un trattamento dati con strumenti elettronici: ad esempio, quando prevista dal sistema di autenticazione informatica, la parola chiave (password) dovrà essere composta da almeno 8 caratteri o da un numero di caratteri pari al massimo consentito. La password non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata almeno ogni 6 mesi; nel caso di trattamento di dati sensibili – come nell'ambito sanitario – tale intervallo temporale si riduce a 3 mesi. Un grande esperto di security statunitense affermava che la password è assimilabile ad uno spazzolino da denti: va usato tutti i giorni e cambiato spesso. Ovviamente la password non deve essere per alcun motivo divulgata.

Un altro punto molto importante riguarda le credenziali di autenticazione che non possono, in caso di inutilizzo, essere assegnate ad altri Incaricati, neppure in tempi diversi. Se non vengono utilizzate per almeno 6 mesi o in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati (verifica almeno annuale della sussistenza delle condizioni per la conservazione dei profili di autorizzazione!), tali credenziali devono essere disattivate.

Come disposto dal Disciplinare Tecnico, il Titolare o il Responsabile devono impartire specifiche istruzioni agli Incaricati onde evitare di lasciare incustodito o comunque accessibile lo strumento elettronico durante la sessione di trattamento: si tratta molto semplicemente di avere cura della propria stazione di lavoro, adoperandola e custodendola con attenzione. I monitor dei computer rappresentano una finestra aperta su archivi e dati che possono essere consultati solo da soggetti preventivamente autorizzati. Un comportamento superficiale nei confronti di tali strumenti può dar luogo a situazioni pericolose con il rischio di conseguenze (anche penali!) per colui che consente l'illecito accesso ai dati personali che gli sono stati affidati per scopi di lavoro. E' pertanto necessario adottare una condotta consapevole chiudendo a chiave l'ufficio o lo studio in cui siano presenti computer o materiale cartaceo contenente dati personali e sensibili durante le assenze, anche per brevi periodi.

La postazione di lavoro va costantemente presidiata evitando di lasciare il computer collegato alla rete quando non è strettamente necessario, utilizzando screensaver e altri analoghi software che consentano il blocco della tastiera e dello schermo in caso di inattività della stazione di lavoro, chiudendo la sessione quando ci si allontana e controllando eventuali segni di effrazione.



L'Incaricato deve farsi parte attiva della sicurezza dei dati da un lato adottando misure di sicurezza fisica e, dall'altro, non esitando a chiedere al Responsabile o al Titolare gli strumenti necessari per garantirla. Vi è da sottolineare che la normativa prevede comunque l'aggiornamento almeno semestrale o annuale, rispettivamente per i dati sensibili/giudiziari e personali, degli strumenti elettronici, intendendosi ovviamente la componente software.

Ricorda: adotta, formalizza, controlla le misure di sicurezza. Ogni tre mesi cambia la password del tuo computer

Che cosa è il Documento Programmatico per la Sicurezza (DPS)?

Il punto 19 dell'Allegato Tecnico al d.lgs. 196/2003 stabilisce l'obbligo da parte dei Titolari che trattino dati sensibili o giudiziari di redigere annualmente un documento che fornisca un idoneo ed esaustivo quadro della situazione in tema di sicurezza e privacy. Nello specifico tale documento deve contenere l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità, l'analisi dei rischi, le misure di sicurezza adottate, la descrizione dei criteri di ripristino di dati cancellati o danneggiati, un piano degli interventi di formazione, i criteri per la sicurezza nei casi di "outsourcing" e per la cifratura o la disgiunzione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati dell'Interessato. Il termine per la stesura del DPS è fissato entro il 31 marzo di ogni anno.

Nel quadro di una gestione strategica della sicurezza, l'analisi dei rischi rappresenta la fase più critica e nel contempo di maggiore importanza poiché attraverso essa vengono definite le priorità con cui devono essere affrontati i possibili rischi. In tale prospettiva l'analisi dei rischi rientra nel più complesso ambito della gestione del rischio (risk management) i cui obiettivi sono rappresentati dalla salvaguardia delle finalità dell'organizzazione e dalla tutela degli utenti. Il risk management deve essere pianificato tenendo in considerazione l'indifferibilità delle iniziative mirate alla salvaguardia del patrimonio informativo, le priorità operative (funzionalità, efficienza ed efficacia dei sistemi per il trattamento dei dati) e, non ultima, la necessità di rispettare un rapporto di economicità delle soluzioni, ricercando un giusto equilibrio tra costi e benefici attesi.

La fase analitica si compone di due distinte sotto-fasi temporalmente consecutive: l'identificazione del rischio e l'assegnazione delle priorità di intervento a fronte dei rischi identificati e analizzati. Nella fase di gestione vera e propria si passa dalla pianificazione delle attività alla soluzione dei rischi per arrivare infine al monitoraggio di nuove potenziali insidie.

Da tutto ciò consegue come nelle grandi organizzazioni il Titolare per redigere il DPS debba necessariamente avvalersi dell'aiuto del/dei Responsabile/i e di alcuni Incaricati che meglio conoscono la singola realtà operativa e conseguentemente i rischi correlati alla sua attività.

Sono previste delle sanzioni per chi sbaglia?

Il Codice della Privacy prevede sanzioni particolarmente severe per chi non si attiene agli adempimenti prescritti.

Alcuni esempi: chi non rispetta l'adozione delle misure minime di sicurezza previste dall'Art. 33 viene punito con l'arresto sino a 2 anni oppure con un'ammenda da 10.000 a 50.000 Euro.

L'omissione o l'inidoneità dell'informativa viene punita con una sanzione amministrativa variabile dai 3.000 ai 18.000 Euro, eventualmente triplicabile in base al reddito dell'Interessato.

Conclusioni

L'introduzione del Codice della Privacy ha determinato una vera e propria rivoluzione in tutti i settori della società civile ma a tutt'oggi, soprattutto per quanto riguarda le Pubbliche Amministrazioni, l'applicazione delle sue disposizioni è ancora piuttosto lacunosa e incompleta. Nel campo delle aziende sanitarie pubbliche e private ciò è aggravato dall'evidente constatazione che in tale contesto la quasi totalità degli operatori impegnati utilizza, per le specifiche attività di competenza, informazioni delicate da gestire, come quelle relative allo stato di salute (dati sensibili), nei confronti delle quali la legge prevede una tutela maggiore.

Considerato l'impatto trasversale del Codice della Privacy ed il fatto che in ogni settore e servizio di un ente o di una organizzazione complessa, come può essere un'azienda sanitaria, vengono svolte operazioni di trattamento, anche se non espressamente previsto dalla normativa, nasce l'esigenza di creare un organismo che abbia una visione di insieme delle attività svolte e da svolgere. Alcune Amministrazioni hanno provveduto ad istituire un apposito gruppo di lavoro, il cosiddetto *Gruppo Privacy*, costituito da diverse professionalità (sanitarie, amministrative, tecniche, ecc). Il Gruppo Privacy, che deve necessariamente operare in posizione di staff con gli organi di vertice, ha il compito di effettuare un monitoraggio dei trattamenti, un aggiornamento delle procedure, la segnalazione delle novità normative e, non meno importante, un'opera di formazione ed informazione, al fine di sostenere la nascita e la crescita di una cultura del rispetto della riservatezza a livello aziendale. I dati raccolti in sede di monitoraggio devono essere utilizzati per predisporre la modulistica necessaria (informativa, lettere di incarico, notifica al Garante) e per adempiere agli altri obblighi previsti dalla legge. Inoltre, il Gruppo Privacy deve procedere all'attività di *auditing*, verificando la corrispondenza e la correttezza delle attività esercitate rispetto a quanto previsto in sede normativa.

Il Gruppo Privacy ed altri strumenti consentono di interpretare nel modo corretto il Codice permettendo di modificare il proprio *modus operandi* consolidato nel tempo, sostenere il cambiamento, revisionare i propri flussi informativi sia interni che esterni, riorganizzare la gestione delle informazioni, mettere in sicurezza i propri archivi e le informazioni trattate. In tal modo il Codice della Privacy non rappresenta più solo un insieme di norme ed un ulteriore fardello burocratico ma diventa vero e proprio strumento della qualità e può contribuire a quel "salto culturale" che da molti è considerato indispensabile, affinché il diritto alla protezione dei dati diventi patrimonio di tutti.

Riferimenti bibliografici

1. Privacy in Pratica. Umberto Rapetto e Barbara Rapetto Freddi. EPC Libri, 2003.
2. La tutela della privacy in ambito socio-sanitario. Fabio Trojani. Maggioli Editore, 2002.
3. Codice della Privacy e misure minime di sicurezza. II edizione. Adalberto Biasiotti. EPC Libri, 2004.
4. Il Sole 24 Ore. Anno 140, numero 82, pag. 29.
5. Il diritto alla protezione dei dati personali. Riccardo Acciai. Maggioli Editore, 2004.
6. Sito web: www.privacy.it.
7. Sito web: www.garanteprivacy.it

Le *"Formiche della Privacy"* sono di Fabio Vettori, Grafico in Trento.
Per saperne di più visita il sito *www.fabiovettori.com*

Si ringrazia il Sig. Gualtiero Marini, Tecnico Coordinatore dell'Unità Operativa di Radiologia dell'Ospedale Santa Chiara di Trento, per la preziosa collaborazione.