



Dr. iur. Michele Albertini
Residenza governativa
Via Canonico Ghiringhelli 1
6501 Bellinzona

segretariato 091 814 45 02
fax 091 814 45 09
E-Mail protezionedati@ti.ch
Web www.ti.ch/protezionedati

Sicurezza: tra privacy e qualità delle cure

Traccia della relazione del 12 settembre 2007 al 3° simposio cantonale di Rete sanitaria “Sanità elettronica: più sicurezza per tutti”, Forum salute Ticino, Lugano

È determinante esclusivamente il testo esposto e sviluppato oralmente

Indice

1. Introduzione
2. Privacy e qualità delle cure: due obiettivi in conflitto?
 - 2.1. Stato di salute e senso di privacy
 - 2.2. Il ruolo attivo dell'operatore sanitario nella tutela degli interessi del paziente
 - 2.3. Significato della protezione dei dati nell'era della sanità elettronica
3. Sicurezza dei dati: un valore imprescindibile
 - 3.1. Sanità elettronica ed esigenze di sicurezza
 - 3.2. Sicurezza modulata
4. Conclusione
5. Riferimenti

1. Introduzione

Signore e signori,

ho raccolto con interesse l'invito a formulare qualche breve considerazione, dall'osservatorio della protezione dei dati, su alcuni quesiti, niente affatto teorici, che concernono il rapporto tra il cittadino (nella sua qualità di paziente) e chi lo cura (essenzialmente il medico e i suoi ausiliari, rispettivamente la struttura ospedaliera).

Nell'epoca della sanità elettronica, con le sue immense opportunità ma anche con i suoi rischi potenziali, può l'esigenza di tutelare la privacy ostacolare la qualità delle cure? All'inverso, l'esigenza di assicurare la qualità più elevata possibile delle cure, in particolare mediante l'uso della tecnologia nella condivisione della presa a carico tra più attori, in contemporanea e in luoghi diversi, compromette la tutela della privacy?

Così formulati, i quesiti sembrano porre il paziente davanti ad un vero e proprio dilemma: perché sia garantito un valore, egli deve rinunciare all'altro. Detto altrimenti: la necessità di tutelare la riservatezza si contrappone all'esigenza di garantire le migliori cure possibili. E viceversa.

Ma è veramente corretto porre questi valori sullo stesso piano? Ed è giusto, soprattutto, ritenerli in conflitto, come si potrebbe anche essere indotti a credere? In queste brevi annotazioni vorrei contribuire a sfatare il malinteso e convincere del fatto che la protezione dei dati, se ben concepita ed attuata nell'era della sanità elettronica – soprattutto nell'ottica della promozione della sicurezza – non ostacola affatto la presa a carico ma, al contrario, concorre a migliorarne l'efficacia.

2. Privacy e qualità delle cure: due obiettivi in conflitto?

Sappiamo che la protezione dei dati è anzitutto un *diritto* del cittadino, sancito dalla costituzione e precisato dalla legge. Le norme sulla protezione dei dati non si limitano però ad assicurare, in senso stretto, il diritto di ciascuno di esigere la tutela della riservatezza da parte di professionisti e autorità che trattano dati personali, ma, in modo più ampio, enunciano le regole che questi devono seguire quando impiegano simili informazioni. Queste peculiarità, completate da una serie di strutturati e corollari diritti individuali d'accesso e di controllo, contribuiscono a rendere effettiva la cosiddetta *autodeterminazione informativa del singolo*, ossia il diritto di ciascuno di poter gestire liberamente e in modo autonomo le informazioni che lo riguardano.

Queste prerogative sono di particolare rilievo nell'ambito medico-sanitario, dove sussistono bisogni specifici di assicurare un flusso ordinato di informazioni – tra chi le gestisce e le elabora e la persona interessata – e di provvedere alla loro sicurezza.

La responsabilità di rispettare queste regole, e di adottare le misure adeguate, incombe al professionista (rispettivamente alla struttura), né più né meno della responsabilità di garantire cure di qualità.

E il singolo cittadino – confrontato con la necessità di sottoporsi alle cure – quale ruolo ha in questo processo?

2.1. Stato di salute e senso di privacy

Il paziente cagionevole di salute vuole guarire: e per guarire nel modo migliore è disposto – le esperienze lo insegnano – a condividere e a far condividere con gli operatori sanitari tutta una serie di dati anche di natura estremamente sensibile, per certi versi dando loro carta bianca, senza valutare (sempre) le conseguenze dirette e indirette del modo di gestione (corretto, lacunoso o addirittura illecito) delle informazioni. La persona sana, invece, questa preoccupazione non l'ha, o meglio non la sente. Del tutto naturalmente tende a privilegiare la privacy, secondo il valore soggettivo che usualmente le attribuisce.

È innegabile che lo stato di salute influenza o quanto meno possa influenzare – di fatto – il valore che il singolo paziente attribuisce alla protezione dei dati. Questa minore “attenzione” (se così si può dire) da parte sua non dev'essere una ragione perché l'operatore sanitario la ignori o ne banalizzi la portata. Al contrario.

2.2. Il ruolo attivo dell'operatore sanitario nella tutela degli interessi del paziente

Come per la ricerca della migliore presa a carico possibile, l'operatore sanitario deve – sulla base del particolare rapporto di fiducia esistente tra le parti (specialmente quando lo stato di salute del paziente è cagionevole) – farsi garante degli interessi del paziente anche in merito alla protezione dei dati e alle norme di comportamento che concorrono ad attuarla. L'importanza della tutela degli interessi del paziente è peraltro ribadita anche nella nuova legge federale sulle professioni mediche universitarie, entrata in vigore il 1° settembre scorso.

Il discorso è importante da sempre, e lo è ancora di più nell'era della sanità elettronica, considerate le sue implicazioni dirette e indirette, le sue opportunità e i suoi rischi.

2.3. Significato della protezione dei dati nell'era della sanità elettronica

Gli obiettivi fondamentali della sanità elettronica sono molteplici e tutti positivi nell'ottica della presa a carico del paziente: miglioramento dell'efficacia e della qualità delle cure, diminuzione dei rischi d'errore, accrescimento della produttività e diminuzione dei costi, incremento della coordinazione e della sicurezza, e così via.

Le *opportunità e potenzialità* offerte dall'uso delle tecnologie dell'informazione e della comunicazione sono evidenti alla luce dei nuovi strumenti e applicazioni della strategia di sanità elettronica: si pensi in modo particolare al *dossier elettronico del paziente, personale e per tutta la vita* (dal 2015, con gradualità preparatori a partire dal prossimo anno), come pure le *informazioni e servizi online* (gradualmente dal 2008, fino a giungere, nel 2015, all'accesso ad informazioni strutturate, accreditate e specifiche nel dossier elettronico del paziente). Si pensi poi agli strumenti, per così dire complementari, d'identificazione, e non solo: la *tessera d'assicurato* (che sarà introdotta nel 2009 e che permetterà la memorizzazione facoltativa di dati sanitari di una certa rilevanza per il trattamento medico), e la *tessera del professionista della sanità* (prevista dal prossimo anno per decisione della FMH, e che consentirà ai medici di trasmettersi più facilmente le informazioni sullo stato di salute di pazienti).

In definitiva la visione, che diventerà realtà, è la seguente: tutti i cittadini potranno mettere le proprie informazioni personali a disposizione di tutti gli operatori sanitari di loro scelta, e di beneficiare di prestazioni. In questo senso, gli strumenti della sanità elettronica possono assicurare maggiore qualità e sicurezza dell'informazione medico-sanitaria di quanto consentano le forme tradizionali di documentazione.

La conseguenza, inevitabile e irrinunciabile, è però anche questa: maggiori sono i servizi sanitari offerti, maggiori e più complessi sono i dati trattati, che devono essere disponibili sempre più in fretta e nel luogo dove sono richiesti, ad una cerchia più ampia di interessati. Ciò introduce nuovi scenari di *rischi*, non sempre palesi, ma accresciuti quando si parla di elaborazioni informatiche o quando le informazioni sono messe in rete, indipendentemente dagli strumenti di sanità elettronica. In più, la *manca di consapevolezza* dell'esistenza di tali rischi può contribuire a banalizzare molti problemi e a prospettare nuove possibilità di abuso.

Per queste ragioni, descritte in modo forzatamente sintetico, la protezione dei dati assume e deve assumere un ruolo guida nella definizione, a priori, di standard e di regole di comportamento da parte degli operatori sanitari, oltre che presiedere alla sicurezza (tecnica) del trattamento delle informazioni.

Nell'ambito della sanità elettronica vi sono temi tipici che vanno affrontati e risolti in modo adeguato. In particolare occorre definire regole e modalità precise in merito all'informazione del paziente (strutturata o semplificata) e al suo consenso (esplicito e preventivo o nella forma del silenzio-assenso), quali elementi cardini dell'autodeterminazione, ribadire il ruolo determinante dell'operatore sanitario nella tutela degli interessi del paziente, stabilire parametri chiari di accessibilità alle informazioni e relativi limiti, predisporre regole di identificazione (degli operatori sanitari e dei pazienti) e di gestione delle informazioni con riguardo anche alle misure di carattere tecnico, determinare standard e modalità per il trasferimento di dati, anche all'estero e viceversa (anonimizzazione, pseudonimizzazione ecc.), come pure individuare meccanismi di controllo e di verifica e determinare le regole in caso di usi secondari dei dati (specie per fini di ricerca) e, non da ultimo, verificare e adattare le regole in funzione dello sviluppo tecnologico.

Da qui emerge l'effettiva, dinamica funzione della protezione dei dati nell'era della sanità elettronica: non riveste più solo un ruolo difensivo fondato sulla tutela della personalità, ma persegue un ruolo propositivo, per consentire che solo le informazioni complete e pertinenti siano elaborate e comunicate, e che lo siano, in un quadro di legalità, in modo efficiente, tempestivo e sicuro. Ciò, indiscutibilmente, accresce la qualità delle cure.

3. Sicurezza dei dati: un valore imprescindibile

3.1. Sanità elettronica ed esigenze di sicurezza

Nella strategia della sanità elettronica, la rilevanza della protezione dei dati si identifica in modo significativo con la sicurezza dei sistemi informatici e della trasmissione o condivisione elettronica dei dati, quindi con tutte le misure preposte a garantire il rispetto dei noti principi legali della *confidenzialità*, dell'*integrità*, dell'*autenticità* e della *disponibilità* delle informazioni.

Questi elementi sono ribaditi e sottolineati nelle raccomandazioni del 13 febbraio 1997 del Comitato dei Ministri del Consiglio d'Europa all'indirizzo degli Stati membri relative alla protezione dei dati sanitari (raccomandazione R(97)5), a cui rinvio. Essi sono esposti an-

che nel documento approvato nel febbraio di quest'anno dai Garanti europei per la protezione dei dati, con specifico riferimento alla cartella clinica elettronica; questo testo approfondisce i requisiti di legge e i parametri applicativi da considerare nella strutturazione e nella gestione di un sistema nazionale di cartelle elettroniche.

In estrema sintesi gli operatori sanitari devono adottare adeguate *misure tecniche ed organizzative*, anche individuali, per preservare le informazioni, istruendo adeguatamente il personale. I dati memorizzati ed elaborati elettronicamente possono essere visionati, copiati, modificati e trasmessi solo da persone autorizzate. Queste ultime devono potersi identificare in modo certo e univoco. I sistemi devono garantire che i dati siano disponibili, nella forma e nei contenuti, nel momento richiesto ed assicurare che essi non siano modificati o distrutti (in modo accidentale o illecito). Inoltre occorre poter documentare chi ha immesso, modificato o cancellato quali dati nel sistema e garantire le necessarie procedure e protocolli.

3.2. Sicurezza modulata

Una sicurezza dei dati effettiva deve considerare l'insieme degli elementi della situazione specifica. Le esigenze vanno definite a dipendenza del settore e del contesto dell'elaborazione dei dati, in base al principio – sancito in modo chiaro nella raccomandazione R(97)5 – della *sicurezza modulata*.

Sicurezza modulata significa che le misure devono garantire un livello di sicurezza appropriato, alla luce, da un lato, dello stato della tecnica e, dall'altro, della natura sensibile dei dati trattati e della valutazione dei rischi potenziali. Le misure, che devono essere esaminate periodicamente, dipendono evidentemente anche dal tipo di elaborazione e dal tipo di soggetto interessato (una struttura ospedaliera ha caratteristiche diverse rispetto ad uno studio medico). Considerate le responsabilità, significative, che incombono alle strutture che gestiscono sistemi complessi dove sono trattati dati sensibili, soprattutto della sfera medica, è indispensabile che esse adottino un regolamento interno che disciplini le misure tecniche, organizzative, le procedure, il controllo e le persone designate per tali scopi, con le rispettive competenze.

I *fattori essenziali* per una sicurezza modulata possono essere individuati, in particolare, nei seguenti elementi: predisporre un accesso selettivo e modulato, con riguardo anche alle misure di carattere tecnico quali identificazione, autenticazione e autorizzazione, definire una struttura modulare del supporto di dati, che possa permettere la separazione fra le diverse categorie di dati rispetto alle finalità del trattamento e ai soggetti che vi ac-

cedono (elaborazione separata dei dati a dipendenza della loro tipologia, ad esempio gli identificativi e i dati relativi all'identità delle persone, i dati amministrativi, i dati medico-sanitari in senso stretto, ecc.) e, inoltre, determinare i meccanismi di controllo e di verifica a dipendenza del tipo di trattamento delle informazioni, predisponendo un sistema di registrazione e documentazione di tutte le fasi dell'elaborazione.

Una gestione irreprensibile e trasparente delle informazioni, all'insegna di regole chiare e praticabili, è una premessa indispensabile del rapporto di fiducia reciproca tra gli attori sanitari e il paziente.

4. Conclusione

Le mie conclusioni sono brevi. Posso limitarmi a citare una recente affermazione del vicepresidente Garante italiano per la protezione dei dati personali, che condivido pienamente¹: *"Lo sviluppo delle nuove tecnologie dell'informazione e della comunicazione in campo sanitario esprime l'esigenza inderogabile di conciliare il valore dell'efficienza con l'altrettanto fondamentale valore della tutela della riservatezza dei cittadini. Il sistema di sanità elettronica, ancor più di altri, deve essere in grado di ingenerare la fiducia dei cittadini"*.

Nell'era della sanità elettronica la protezione e la sicurezza dei dati sono elementi irrinunciabili al buon funzionamento del sistema socio-sanitario che deve poggiarsi, in primo luogo, sulla *fiducia reciproca* tra attori sanitari e strutture, e i pazienti, con particolare riferimento ad una gestione irreprensibile delle informazioni. Se questa mutua fiducia non è data, o è incrinata, sono in pericolo l'efficacia e la sicurezza terapeutica nel singolo caso, la qualità delle cure e, in definitiva, il perseguimento dello stesso interesse pubblico alla tutela e alla promozione della salute.

Vi ringrazio.

¹ GIUSEPPE CHIARAVALLI, intervento al Convegno dedicato alle nuove tecnologie dell'informazione e della comunicazione, "Una rete per la salute", Forum della Pubblica amministrazione 2006, Roma 11 maggio 2006.

5. Riferimenti

SVIZZERA

UFFICIO FEDERALE DELLA SANITÀ PUBBLICA

Strategia “eHealth” Svizzera, documento del 27 giugno 2007
(disponibile finora solo in lingua tedesca)

<http://www.bag.admin.ch> → Temi → Assicurazione malattie → Progetti → eHealth

INCARICATO FEDERALE DELLA PROTEZIONE DEI DATI E DELLA TRASPARENZA

▪ Guida al trattamento dei dati personali nella sfera medica

<http://www.edoeb.admin.ch> → Temi → Protezione dei dati → Salute

▪ La protezione dei dati negli studi medici – Interfacce e provvedimenti utili

<http://www.edoeb.admin.ch> → Temi → Protezione dei dati → Salute

→ La protezione dei dati negli studi medici

▪ FAQ Salute (cartelle cliniche e diritto alle informazioni, obbligo del segreto professionale, fatture del medico e per i premi, raccolta di dati medici, altre domande)

<http://www.edoeb.admin.ch> → Documentazione → Protezione dei dati → FAQ → Salute

PRIVATIM – GLI INCARICATI SVIZZERI PER LA PROTEZIONE DEI DATI

Votre dossier médical – Vos droits

(opuscolo disponibile finora solo in lingua tedesca e francese, in allestimento in lingua italiana)

<http://www.privatim.ch>

RESPONSABILE PER LA PROTEZIONE DEI DATI DEL CANTONE TICINO

Cartella sanitaria: diritti individuali e protezione dei dati, in: Diritto senza devianza, studi in onore di Marco Borghi, ed. speciale della Rivista ticinese di diritto 2006, pag. 5-67

<http://www.ti.ch/protezionedati> → pubblicazioni

CONSIGLIO D'EUROPA

COMITATO DEI MINISTRI

Recommandation n. R (97) 5 aux États membres relative à la protection des données médicales, adottata il 13 febbraio 1997, e Exposé des motifs
(entrambi i documenti in lingua francese)

<http://www.coe.int> → Affaires juridiques → Coopération juridique → Protection des données
→ Instruments juridiques internationaux → Recommandations et résolutions du Comité des Ministres

UNIONE EUROPEA

EU HEALTH POLICY – PORTALE E-HEALTH DELL'UNIONE EUROPEA

<http://www.ehealthnews.eu>

ARTICOLO 29 – GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), adottato il 15 febbraio 2007

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_it.pdf