Ricetta elettronica e certificati on line: analisi giuridica in ottica sicurezza e privacy

Chiara Rabbito [1]

[1] *Studio Legale Rabbito, San Lazzaro (Bologna)*

ABSTRACT

The objective of the digitization of the medical prescriptions and certificate takes shape in our legislative system through complex rules, disseminated in a variety of interventions. The author of this article discusses in detail the legislation on electronic prescribing, since Decree Law. 269 of 30 September 2003 up to the data protection code. In addition to the electronic prescription by the family doctor, the author also presents the legal regulations concerning the issuance of medical certificates to be sent via Internet to the administrative control agency and to employer.

The data protection code is a fundamental point, especially for the obligations imposed on the general practitioner regarding the information to be signed by the patient and the ownership of the data requested. Given the sensitivity of the data processed, security must be particularly ensured.

The author finally illustrates the creation of databases in the health sector, emphasizing that it is an operation of extreme importance in terms of privacy, therefore should be paid great attention to the use of security measures.

Keywords: Data protection code; Electronic prescribing; General Practitioner; Privacy

Medical electronic prescriptions and certificates online: legal analysis on security and privacy

Pratica Medica & Aspetti Legali 2015; 9(3): 81-88

http://dx.doi.org/10.7175/pmeal.v9i3.1199

Corresponding author
Chiara Rabbito
info@avvocatorabbito.it

Disclosure
L'autore dichiara di non avere conflitti di interesse di natura finanziaria in merito ai temi trattati nel presente articolo

IL QUADRO NORMATIVO E REGOLAMENTARE

L'obiettivo della digitalizzazione della ricetta e del certificato medico prende forma nel nostro ordinamento attraverso una normazione complessa, disseminata in una molteplicità di interventi e, nei suoi esordi, piuttosto datato.

Il primo atto di questo articolato percorso va ricondotto al decreto legge n. 269 del 30 settembre 2003, intitolato «Disposizioni urgenti per favorire lo sviluppo e per la correzione dell'andamento dei conti pubblici» [1], convertito con emendamenti nella legge n. 326 del 24 novembre 2003 [2].

Si tratta dell'atto normativo che introduce il cosiddetto "Sistema TS", il progetto "Tessera Sanitaria". Nello specifico, l'art. 50 del decreto 269, intitolato «Disposizioni in materia di monitoraggio della spesa nel settore sanitario e di appropriatezza delle prescrizioni sanitarie», si prefigge il contenimento della spesa sanitaria e il miglioramento dell'appropriatezza prescrittiva mediante l'adozione del sistema di controllo previsto.

A questo fine si stabilisce l'introduzione della Tessera Sanitaria, da attribuirsi a tutti i soggetti titolari di codice fiscale.

© SEEd Tutti i diritti riservati

L'originaria disposizione, contenuta nei commi 2 e 3 del citato art. 50, regolamenta la ricetta a lettura ottica: il Ministero dell'Economia e delle Finanze, di concerto con il Ministero della Salute, avrebbe messo a punto i ricettari medici standardizzati, ne avrebbe curato la stampa e la successiva distribuzione alle aziende sanitarie locali.

Questo stesso articolo 50 viene poi fatto oggetto di un'importante modifica da parte del legislatore il quale nel 2006 introduce il comma 5 *bis*: è l'art. 1 comma 810 della legge 27 dicembre 2006, n. 296 [3] che inserisce nell'art. 50 questo ulteriore comma. Si tratta della norma che prevede e disciplina la trasmissione telematica dei dati della ricetta al Ministero dell'Economia e delle Finanze.

Il processo di digitalizzazione dei certificati medici risale anch'esso al decennio scorso, in particolare alla Legge finanziaria del 2005: il comma 149 dell'art. 1 della legge 30 dicembre 2004, n. 311 [4] interveniva a modificare l'art. 2 del decreto legge 30 dicembre 1979, n. 663 [5], convertito in legge, con emendamenti, dall'art. 2 della legge 29 febbraio 1980, n. 33 [6] e in seguito ulteriormente modificato dall'art. 15 della legge 23 aprile 1981, n. 155 [7], stabilendo che: «A decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante trasmette all'INPS il certificato di diagnosi sull'inizio e sulla durata presunta della malattia per via telematica online, secondo le specifiche tecniche e le modalità procedurali determinate dall'INPS medesimo».

A seguire, il già citato comma 5 *bis* dell'art. 50, parallelamente alla previsione dell'invio telematico dei dati della ricetta al Ministero delle Finanze, prescrive l'invio anch'esso telematico delle certificazioni di malattia all'INPS.

Per il concreto conseguimento di entrambi gli obiettivi è previsto il collegamento in rete di tutti i medici del Servizio Sanitario Nazionale (SSN) abilitati dalle Regioni ad effettuare prescrizioni. Tale collegamento dovrà avvenire per il legislatore a partire dal 1° luglio 2007 e secondo le regole tecniche del Sistema Pubblico di Connettività e Cooperazione, avvalendosi, ove possibile, delle infrastrutture regionali esistenti.

A completamento, il Decreto del Presidente del Consiglio dei Ministri del 26 marzo 2008, di «Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296, in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema Pubblico di Connettività» [8], e l'allegato disciplinare tecnico definiscono le modalità per la trasmissione telematica dei dati delle ricette al Ministero delle Finanze, nonché le regole tecniche per l'acquisizione e la trasmissione telematica contenuti nelle certificazioni di malattia all'INPS.

Il decreto del 2008 chiarisce che entrambi questi importanti procedimenti di trasmissione dei dati del cittadino si varranno delle infrastrutture tecnologiche denominate Sistema di Accoglienza Centrale (SAC), di competenza del Ministero dell'Economia e delle Finanze, e Sistema di Accoglienza Regionale (SAR), di competenza regionale.

Qualora la Regione di afferenza del medico disponga del proprio SAR, il medico si varrà di questo per l'invio. Nel caso in cui invece la Regione sia sprovvista del SAR, l'invio dei dati avverrà attraverso il Sistema Centrale, gestito da SOGEI, società di Information Technology del Ministero dell'Economia e delle Finanze.

Nel primo caso sarà compito della Regione definire le modalità di raccolta dei documenti e inviare i documenti raccolti dal SAR al SAC. Nel secondo caso, il SAC mette a disposizione degli utenti servizi applicativi per la raccolta e la registrazione dei documenti pervenuti.

La trasmissione a Ministero dell'Economia e delle Finanze e INPS, nell'ambito del SAC, avviene attraverso un servizio di cooperazione applicativa, secondo le regole tecniche del Sistema Pubblico di Connettività e Cooperazione (SPCC).

Per quanto concerne l'invio telematico dei certificati medici nel settore pubblico, l'art. 55 *septies* del decreto legislativo 165 del 2001 [9], introdotto dall'art. 69 del decreto legislativo 150 del 2009 [10], ha determinato l'equiparazione del settore pubblico a quello privato, prevedendo la trasmissione telematica all'INPS dei certificati di malattia anche per i lavoratori del settore pubblico.

A partire dal 3 aprile 2010 i medici dipendenti dal SSN, o in regime di convenzione con esso, sono tenuti a trasmettere il certificato di malattia del lavoratore all'INPS per il tramite del SAC o del SAR.

Il programma di avvio a regime della trasmissione per via telematica delle ricette da parte dei medici prescrittori è stato definito da una serie di decreti ministeriali che ne hanno regolamentato la partenza in base alla Regione di riferimento (decreto ministeriale 14 luglio 2010 [11]; il decreto ministeriale 21 febbraio 2011 [12]; il decreto ministeriale 21 luglio 2011 [13] e infine il decreto ministeriale 2 luglio 2012 [14]).

Con riguardo alla infrastruttura tecnologica di riferimento, il decreto legge n. 78 del 2010 [15], recante «Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica», convertito, con modificazioni, nella legge 30 luglio 2010, n. 122 [16] ha previsto all'articolo 11, comma 16, che ai fini della trasmissione telematica delle ricette mediche, di cui all'articolo 50, commi 4 e 5 del sopra citato decreto legge n. 269/2003 [1], sarà utilizzata la stessa piattaforma messa a disposizione per la trasmissione telematica dei certificati di malattia.

Più specificamente, il citato decreto legge n. 78 del 2010 [15] prevede che, nelle more della emanazione dei decreti attuativi previsti dal decreto legge 269 del 2003 [1], «al fine di accelerare il conseguimento dei risparmi derivanti dall'ado-

© SEEd Tutti i diritti riservati

zione delle modalità telematiche per la trasmissione delle ricette mediche», il Ministero dell'Economia e delle Finanze curi l'avvio della diffusione della suddetta procedura telematica, adottando, in quanto compatibili, le modalità tecniche operative di cui all'allegato 1 del decreto del Ministro della Salute del 26 febbraio 2010 [17], cioè appunto quello relativo ai certificati elettronici.

Lo stesso decreto legge n. 78 del 2010 [15]stabilisce che l'invio telematico dei predetti dati sostituisce a tutti gli effetti la prescrizione medica in formato cartaceo.

In attuazione dell'articolo 11, comma 16, del decreto legge n. 78/2010 [15], il Ministero della Salute e il Ministero dell'Economia e delle Finanze hanno adottato il decreto 2 novembre 2011 [18], con cui sono state definite le modalità tecniche per la dematerializzazione della ricetta medica cartacea, per le prescrizioni a carico del SSN.

Infine, il Decreto Crescita [19], promuovendo l'attuazione dell'Agenda digitale italiana, prevede di accelerare la sostituzione delle prescrizioni mediche di farmaceutica e specialistica a carico del SSN in formato cartaceo con le prescrizioni in formato elettronico. Ai sensi dello stesso decreto, dal 1° gennaio 2014, le prescrizioni farmaceutiche generate in formato elettronico sono valide su tutto il territorio nazionale.

LE CRITICITÀ IN TEMA DI SICUREZZA E PRIVACY: L'INFORMATIVA AL PAZIENTE E LA TITOLARITÀ DEL DATO

Con riguardo alle descritte procedure informatico-telematiche di redazione e spedizione da parte del Medico di Medicina Generale delle ricette e dei certificati digitali dei pazienti, in considerazione della particolare delicatezza dei dati trattati e della complessità e tecnicità delle modalità di trattamento, un primo aspetto meritevole di approfondimento riguarda l'opportunità della predisposizione a beneficio del paziente di un'informativa privacy adeguatamente chiara e completa, che lo renda veramente edotto circa le modalità di trattamento dei suoi dati e i rischi connessi a tale trattamento.

A questo proposito, va ricordato che il Codice della Privacy [20] fa oggetto di specifica disciplina l'informativa del Medico di Medicina Generale, ai sensi dell'art. 78, comma 5, intitolato «Informativa del medico di medicina generale o del pediatra», che riporta: «L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica».

Il Medico di Medicina Generale è dunque tenuto a curare particolarmente il contenuto dell'informativa privacy che sottopone al paziente, con specifico riguardo al caso in cui il trattamento del dato avvenga con modalità tali da accrescere i rischi connessi al trattamento stesso. E l'impiego di procedure informatico-telematiche è sicuramente una delle modalità di gestione del dato che richiedono particolare cautela, in ragione dell'accrescersi dei pericoli per la privacy che esse comportano. Sul punto concordano il legislatore e la nostra Autorità Garante per la privacy.

Da parte sua il legislatore si è sentito in dovere di inserire la specificazione, di cui al sopra citato articolo, con cui si chiede al Medico di Medicina Generale di «evidenziare analiticamente» nell'informativa eventuali trattamenti che si verifichino nell'ambito della telemedicina e della teleassistenza e comunque per «fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica».

Sulla base della lettera della norma sembra quindi opportuno comprendere nei casi da «evidenziare analiticamente» anche le nuove e delicate procedure di invio dei dati della ricetta al Ministero delle Finanze e dei dati del certificato medico all'INPS.

Dell'informativa privacy che il medico deve fornire al paziente si occupa anche il nuovo Codice di deontologia medica [21], il cui art. 78 rubricato «Tecnologie informatiche», riporta: «Il medico, nell'uso degli strumenti informatici, *garantisce l'acquisizione del consenso, la tutela della riservatezza, la pertinenza dei dati raccolti* e, per quanto di propria competenza, la sicurezza delle tecniche. Il medico, nell'utilizzo delle tecnologie dell'informazione e della comunicazione a fini di prevenzione, diagnosi, cura o sorveglianza clinica, o tali da influire sulle prestazioni dell'uomo, si attiene ai criteri di proporzionalità, appropriatezza, efficacia e sicurezza, nel rispetto dei diritti della persona e degli indirizzi applicativi allegati».

Sorgerebbe quindi in capo al Medico di Medicina Generale un obbligo non solo normativo ma anche deontologico circa la necessità della redazione di una informativa per la raccolta del consenso del paziente idonea allo scopo, chiara e adeguatamente dettagliata al fine di consentire all'assistito di esprimere un consenso effettivamente informa-

© SEEd Tutti i diritti riservati

to circa le modalità e le finalità di trattamento dei suoi dati mediante sistemi informatico-telematici.

Con riguardo al grado di «effettiva informazione» del paziente non si possono tuttavia tacere due osservazioni, la prima di tipo generale, la seconda relativa al caso in esame.

In linea generale, va osservato che la comprensione da parte del paziente delle modalità e delle procedure informatiche di trattamento dei suoi dati non potrà essere paragonabile a quella di un esperto del settore, non potrà certo raggiungere un livello di penetrazione e dettaglio circa le criticità e i rischi pari a quello che potrebbe essere afferrato da un tecnico informatico. Si tratterà piuttosto di porsi un obiettivo di "comune" comprensione dei problemi, di un livello medio di conoscenza, quello proprio di un ideale "cittadino tipo". Corrispondentemente ne sarà definito l'obbligo giuridico del medico: non si potrà pretendere che egli renda edotti i propri pazienti fornendo loro complesse nozioni di informatica e di telematica, l'informativa privacy non potrà trasformarsi in un trattato tecnico-scientifico.

D'altro canto l'impossibilità di pretendere che il cittadino medio si trasformi in un esperto in molti settori non fa venire meno il suo diritto giuridicamente riconosciuto ad essere informato.

Con riguardo al caso di specie, cioè con riguardo alla digitalizzazione di ricette e certificati e al loro trattamento mediante il complesso sistema SAC-SAR, oltre al citato limite circa l'approfondita comprensione che del SAC-SAR si possa richiedere al paziente medio, ci sono altri interrogativi che si pongono all'attenzione.

In primis la fonte dell'informazione al paziente.

Come si è detto, il trattamento delle informazioni del paziente mediante il SAC-SAR è stato previsto e disciplinato dal legislatore a fini di controllo di spesa e di programmazione economica. Pertanto se è ovvio che la redazione delle ricette ha quale primaria finalità la salute del cittadino, la particolare modalità di trattamento dei dati sopra descritta pare avere piuttosto un fine più vasto e connesso alle funzioni di governo e amministrative dello Stato: quello relativo alla gestione della spesa sanitaria o, con riguardo al certificato di malattia, della spesa pubblica in generale. Si pone pertanto l'interrogativo se sia il Medico di Medicina Generale che debba approfondire nella informativa privacy che rende al paziente questo particolare tipo di trattamento o se questo compito spetti piuttosto a quegli stessi organi pubblici che a tale trattamento sovraintendono.

Va ricordato, con riguardo a questo aspetto, che la disciplina del dato a contenuto sanitario cambia a seconda della finalità per cui esso è trattato e a seconda dei soggetti che lo trattano.

Il dato a contenuto sanitario è «dato sanitario», e quindi sottoposto alla relativa regolamentazione (artt. 75 e segg. del Codice della Privacy [20]), qualora esso sia trattato a fini di tutela della salute del singolo, di terzi o della collettività e da parte di organismi sanitari o esercenti professioni sanitarie. Qualora invece manchi uno dei citati requisiti (il dato non è trattato a fini di tutela della salute, ma per esempio di controllo della spesa pubblica e/o non è trattato da organismi o professionisti sanitari) esso non è «dato sanitario», ma «dato sensibile», soggetto ai relativi articoli del Codice.

Nel caso del certificato e della ricetta digitali, i dati in essi contenuti trattati mediante il sistema SAC-SAR da parte del Ministero delle Finanze e dell'INPS a fini di controllo di spesa non sono giuridicamente qualificabili come dati sanitari, bensì come dati sensibili. L'interrogativo che si pone è: la descrizione di tale trattamento dovrà entrare a far parte del contenuto di un'informativa fornita da un professionista sanitario (il Medico di Medicina Generale) che tratta invece quei dati a fini di tutela della salute? E per il quale invece quei dati sono dati sanitari in senso proprio?

La questione merita di approfondimento in quanto pare inadeguato far ricadere su un soggetto un obbligo informativo relativo a finalità e mezzi che non gli sono propri.

A nostro giudizio tale obbligo informativo si ferma al trattamento che il medico fa di quei dati con i propri mezzi (quindi entro i limiti del sistema informatico-telematico del suo studio) e per le proprie finalità. Il "passaggio di stato" di quelle stesse informazioni da dati sanitari a dati sensibili fa sì che, nel momento in cui si verifica, e cioè a partire da quando tale trattamento avviene a fini di controllo e gestione di spesa e da parte di soggetti pubblici non sanitari, ad essi debba essere applicata la relativa disciplina prevista dal Codice. Essa prevede che il trattamento dei dati sensibili da parte di soggetti pubblici debba essere dettagliatamente regolamentato dal legislatore (si vedano in proposito i commi 1, 2 e 3 dell'art. 20 del Codice della Privacy [20]) e che i soggetti pubblici che effettuano tale trattamento debbano fornire all'interessato idonea informativa ex art. 13 (art. 22 comma 2) [20]. Il trattamento dei dati sensibili da parte di soggetti pubblici non richiede però, data la natura del soggetto che li tratta e le sue finalità, il consenso dell'interessato. Discende da ciò un'importante conseguenza: anche ammettendo che il soggetto pubblico che tratta per sue finalità di governo i dati del cittadino, e su cui primariamente ricade la responsabilità informativa del cittadino stesso, deleghi in parte e con il suo consenso tale ruolo di informazione al medico, l'informativa privacy del medico si troverà ad avere una natura genetica e funzionale duplice: da una parte si tratterà dell'informativa relativa ai dati sanitari trattati dal medico per la salute del paziente e in relazione ai quali va raccolto il consenso, e dall'altra di una informativa che il medico presenta in quanto "rappresentante" del soggetto

© SEEd Tutti i diritti riservati

pubblico che tratta i dati per finalità di governo e in relazione al cui trattamento il consenso del paziente non va raccolto.

In ogni caso, sulla base dell'analisi giuridica, il ruolo di «titolare dei dati» con riguardo ai dati trattati a scopo di controllo e gestione della spesa pubblica o, più genericamente, a scopo amministrativo e di funzione pubblica va riconosciuto ai soggetti pubblici cui quei dati sono inviati, cioè il Ministero delle Finanze e l'INPS.

Va ricordato infatti che per «titolare dei dati» ai sensi dell'art. 4 comma 1 lett. f del Codice Privacy [20], deve intendersi «la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».

Sotto questo profilo desta perplessità quanto previsto dal Disciplinare tecnico del decreto del Ministero delle Finanze 27 luglio 2005 [22], disciplinante i «parametri tecnici per la realizzazione del software e modalità di trasmissione dei dati delle ricette al Ministero dell'Economia e delle Finanze». In particolare tale decreto indica i Medici di Medicina Generale quali «utenti»: ad essi è rivolto il servizio telematico, sono individuati all'interno di ciascuna struttura sanitaria accreditata e devono essere preventivamente autorizzati dal Ministero dell'Economia e delle Finanze.

Fin qui *nulla quaestio*. Ciò che lascia perplessi è la loro definizione quali «titolari del trattamento» ai sensi del Codice della Privacy: il punto 1.5, rubricato «Trattamento dei dati e obbligo di riservatezza» precisa infatti: «Gli utenti delle strutture sanitarie accreditate possono pertanto trattare i dati contenuti nelle ricette per la sola finalità di servizio della trasmissione telematica. *Gli utenti si configurano quali autonomi titolari del trattamento dei dati personali ai sensi dell'art. 4. Comma 1 lett. f del d. lgs. 2003, n. 196*» [22].

Sulla base di quanto precedentemente illustrato pare azzardata – con riguardo a tutto il complesso sistema di ricetta dematerializzata legislativamente previsto –, l'attribuzione al medico del ruolo di titolare, non avendo egli né poteri decisionali relativamente alle finalità di trattamento dei dati né possibilità di controllo circa le loro modalità di trattamento, circa il livello di sicurezza adottato e circa il loro destino.

Al medico si può piuttosto attribuire la natura di «responsabile», ovvero di colui che, preposto dal titolare, deve seguirne le istruzioni e attenersi alle indicazioni date, mentre la caratteristica della titolarità andrà piuttosto riconosciuta ai soggetti pubblici di vertice deputati alla gestione del complesso sistema SAC-SAR e al trattamento dei dati per le finalità pubbliche di buon governo e di controllo di spesa.

NECESSITÀ DEL RISPETTO DEI REQUISITI PREVISTI PER LA COSTRUZIONE DELLE BANCHE DATI

In relazione ai descritti procedimenti deve essere particolarmente curato, data la delicatezza dei dati trattati, il profilo della sicurezza.

L'art. 2 del decreto del Presidente del Consiglio dei Ministri del 26 marzo 2008, intitolato «Trattamento dei dati e obbligo di riservatezza» riporta: «La riservatezza dei dati e dei documenti informatici scambiati nell'ambito del SAC viene garantita dalle procedure di sicurezza relative al software e ai servizi telematici, in conformità alle regole tecniche di cui all'art. 71, comma 1-bis, del Codice (dell'Amministrazione Digitale)» [8].

È pertanto opportuno che i sistemi di elaborazione e di memorizzazione dei dati si caratterizzino per chiarezza e massima tutela del dato, ciò sia con riferimento alla memorizzazione dei dati nel o negli archivi elettronici dello studio medico, quanto con riferimento a tutti i successivi punti di elaborazione e memorizzazione del dato nell'impianto SAC-SAR.

Sotto questo profilo vanno ricordati i requisiti cui devono sottostare le banche dati contenenti dati sensibili e/o sanitari ai sensi del Codice Privacy [20].

La creazione di data base sanitari è un'operazione di estremo rilievo sotto il profilo del rispetto della normativa privacy e va posta grandissima attenzione all'impiego delle misure di sicurezza. La grande rilevanza che il legislatore attribuisce alla tematica è provata dal fatto che il Codice si occupa in più punti della relativa disciplina.

Innanzitutto l'art. 22, comma 6, stabilisce che i dati sensibili (e dunque anche i dati sanitari) contenuti in banche di dati e tenuti con l'ausilio di strumenti elettronici, vanno «trattati con tecniche di cifratura» oppure «mediante l'utilizzazione di codici identificativi o di altre soluzioni» che, considerato il numero e la natura dei dati trattati, «li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità» [20]. L'obiettivo perseguito è, quindi, quello di realizzare una banca dati contenente sì informazioni sanitarie, ma in cui il paziente a cui queste si riferiscono sia riconoscibile solo in caso di necessità. E i modi indicati dal legislatore per conseguire questo risultato sono: tecniche di cifratura, codici identificativi o altro in base alle innovazioni tecnologiche del momento.

Il successivo comma 7 aggiunge: «I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo» [20].

© SE*Ed* Tutti i diritti riservati

Queste precauzioni sono ribadite nella parte dedicata alle misure minime di sicurezza, la cui mancata adozione è penalmente sanzionata. Infatti l'art. 34, relativo ai «Trattamenti con strumenti elettronici»[20], ci dice che è necessario che vengano adottate «tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari».

Se si esaminano congiuntamente gli articoli 22 e 34 [20]pare quindi se ne possa dedurre che nel caso di creazione di banche dati informatizzate contenenti dati sanitari, debbano essere adottate tecniche di cifratura o codici identificativi che consentano di separare l'informazione sanitaria dal nome o dal codice identificativo del paziente e che le informazioni sanitarie (oggetto di particolare tutela) siano separate dagli altri dati personali riferiti al paziente.

Ai sensi del comma 6 dell'art. 22 tale separazione parrebbe predisposta a massima tutela del paziente e cioè affinché il paziente cui il dato sanitario si riferisce non sia immediatamente riconoscibile neppure dall'operatore sanitario autorizzato all'accesso e già autenticatosi.

L'abbinamento dato identificativo-dato sanitario (e quindi la riconoscibilità del paziente) dovrà infatti avvenire solo a seguito di un'ulteriore operazione volontaria e consapevole del sanitario di decifratura o di immissione di codice identificativo.

Quindi a dire che solo se ne ha la volontà e la consapevolezza, il sanitario potrà vedere a chi si riferiscono quelle informazioni sanitarie ed eventualmente integrarle, correggerle o modificarle.

Questa interpretazione delle citate norme sembra confermata da una parte del Disciplinare tecnico in materia di misure minime di sicurezza, Allegato B [20], il cui punto 19.8 richiedeva (è stato infatti recentemente abrogato) che il Documento Programmatico sulla Sicurezza effettuasse «per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato».

Il successivo punto 24 – ancora in vigore – poi prevede, in relazione alle «Ulteriori misure in caso di trattamento di dati sensibili o giudiziari», che: «Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati» [20].

La realizzazione in termini tecnici delle indicazioni del legislatore sembra richiedere una vera e propria progettazione *ad hoc* del data base che dovrà essere creato intorno alla separazione fisica dei dati identificativi rispetto a quelli idonei a rivelare lo stato di salute.

Il *matching* tra i dati identificativi e le informazioni sensibili dovrà poi essere effettuato tramite un codice identificativo univoco del paziente in modalità sicura.

I dati identificativi potranno essere cifrati a livello di data base tramite tecniche avanzate di crittografia: ciò consentirà di mantenere anonimi i dati idonei a rilevare lo stato di salute in caso di accessi non autorizzati al database.

Al fine, poi, di rendere i dati identificativi temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e di rendere possibile l'identificazione degli interessati solo in caso di necessità, come richiesto dal comma 6 dell'art. 22 [20], l'interfaccia grafica del programma dovrà consentire la visualizzazione in forma anonima dei dati idonei a rivelare lo stato di salute dell'interessato al trattamento: i dati identificativi saranno visualizzati in forma cifrata e risulteranno pertanto inintelligibili.

In caso di necessità di utilizzo, l'applicazione dovrà consentire ai soli utenti autorizzati di visualizzare i dati anagrafici in chiaro, mediante loro decifratura.

Il ricongiungimento dei dati clinici e di quelli identificativi a formare il dato sensibile avverrà quindi solamente sull'interfaccia dell'applicazione e solo se necessario: il *matching* tra i due tipi di dati sarà effettuato, come detto, dal codice identificativo del paziente e informazione anagrafica e sanitaria saranno unite solo a livello visivo nell'interfaccia grafica, rendendo così il dato sensibile intelligibile all'utente autorizzato e su sua richiesta.

Un altro aspetto di grande attualità riguarda l'uso del *cloud*: nel caso del trattamento di dati sanitari e sensibili deve essere effettuato con molta prudenza, in considerazione della necessità della massima tutela dei dati sanitari.

Il Garante della privacy italiano ha più volte messo in guardia gli utenti nei confronti di un utilizzo del *cloud* poco oculato e nei confronti di fornitori non adeguatamente diligenti.

In particolare, nel documento «*Cloud computing*: proteggere i dati per non cadere dalle nuvole» [23], il Garante si è raccomandato di fare attenzione ai gestori di servizi intermedi: «Il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri service provider, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati».

Va ricordato, inoltre, che il Codice della Privacy, all'art. 45, limita il trasferimento dei dati nei Paesi extra-europei. Esso recita: «Trasferimenti vietati: 1. Fuori dei casi di cui agli articoli 43 e 44 (cioè dei casi di trasferimenti specificamente consentiti

© SEEd Tutti i diritti riservati

e disciplinati – nota dell'autore), il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza» [20].

Data la delicatezza delle informazioni trattate, nel caso di dati sanitari è quindi consigliabile, a meno di soluzioni tecnologiche ragionevolmente sicure, effettuare il trattamento *in house* e in ogni caso inserire nei contratti clausole che impediscano al *cloud provider* di far risiedere i dati in server collocati in Paesi extra-europei.

BIBLIOGRAFIA

1. Decreto legge 30 settembre 2003, n. 269. Disposizioni urgenti per favorire lo sviluppo e per la correzione dell'andamento dei conti pubblici. Gazzetta Ufficiale n. 229 del 2 ottobre 2003. Suppl. Ordinario n. 157
2. Legge 24 novembre 2003, n. 326. Conversione in legge, con modificazioni, del decreto-legge 30 settembre 2003, n. 269, recante disposizioni urgenti per favorire lo sviluppo e per la correzione dell'andamento dei conti pubblici. Gazzetta Ufficiale n. 274 del 25 novembre 2003. Suppl. Ordinario n. 181
3. Legge 27 dicembre 2006, n. 296. Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007). Gazzetta Ufficiale n. 299 del 27 dicembre 2006. Suppl. Ordinario n. 244
4. Legge 30 dicembre 2004, n. 311. Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2005). Gazzetta Ufficiale n. 306 del 31 dicembre 2004. Suppl. Ordinario n. 192
5. Decreto legge 30 dicembre 1979, n. 663. Finanziamento del Servizio sanitario nazionale nonché proroga dei contratti stipulati dalle pubbliche amministrazioni in base alla legge 1° giugno 1977, n. 285, sull'occupazione giovanile. Gazzetta Ufficiale n. 355 del 31 dicembre 1979
6. Legge 29 febbraio 1980, n. 33. Conversione in legge, con modificazioni, del D.L. 30 dicembre 1979, n. 663, concernente provvedimenti per il finanziamento del Servizio sanitario nazionale, per la previdenza, per il contenimento del costo del lavoro e per la proroga dei contratti stipulati dalle pubbliche amministrazioni in base alla L. 1° giugno 1977, n. 285, sull'occupazione giovanile. Gazzetta Ufficiale n. 59 del 29 febbraio 1980
7. Legge 23 aprile 1981, n. 155. Adeguamento delle strutture e delle procedure per la liquidazione urgente delle pensioni e per i trattamenti di disoccupazione, e misure urgenti in materia previdenziale e pensionistica. Gazzetta Ufficiale n. 114 del 27 aprile 1981
8. Decreto del Presidente del Consiglio dei Ministri 26 marzo 2008. Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296, in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema pubblico di connettività. Gazzetta Ufficiale n. 124 del 28 maggio 2008
9. Decreto legislativo 30 marzo 2001, n. 165. Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche. Gazzetta Ufficiale n.106 del 9 maggio 2001. Suppl. Ordinario n. 112
10. Decreto legislativo 27 ottobre 2009, n. 150. Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni. Gazzetta Ufficiale n. 254 del 31 ottobre 2009. Suppl. Ordinario n. 197
11. Decreto ministeriale 14 luglio 2010. Comunicazione dell'avvio a regime del sistema regionale della regione Lombardia, per la trasmissione telematica dei dati delle ricette a carico del Servizio sanitario nazionale da parte dei medici prescrittori regionali. Gazzetta Ufficiale n. 176 del 30 luglio 2010
12. Decreto 21 febbraio 2011. Avvio a regime del sistema di trasmissione telematica dei dati delle ricette del SSN da parte dei medici prescrittori, presso le regioni Valle d'Aosta, Emilia Romagna, Abruzzo, Campania, Molise, Piemonte, Calabria, Liguria, Basilicata e la provincia Autonoma di Bolzano. (11A02987). Gazzetta Ufficiale n. 53 del 5 marzo 2011
13. Decreto ministeriale 21 luglio 2011. Trasmissione telematica delle ricette del servizio sanitario nazionale da parte dei medici prescrittori e la ricetta elettronica (Progetto Tessera Sanitaria). Avvio a regime del Sistema presso le Regioni Toscana, Puglia, Sardegna e la provincia autonoma di Trento. (11A10623). Gazzetta Ufficiale n. 183 dell'8 agosto 2011
14. Decreto ministeriale 2 luglio 2012. Avvio a regime delle procedure per la trasmissione telematica dei dati delle ricette a carico del Servizio sanitario nazionale da parte dei medici prescrittori regionali e ricetta elettronica presso le regioni Veneto, Friuli-Venezia Giulia, Umbria, Marche, Lazio e Sicilia. Gazzetta Ufficiale n. 160 dell'11 luglio 2012
15. Decreto legge 31 maggio 2010, n. 78. Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica. (10G0101). Gazzetta Ufficiale n. 125 del 31 maggio 2010. Suppl. Ordinario n. 114
16. Legge 30 luglio 2010, n. 122. Conversione in legge, con modificazioni, del decreto-legge 31 maggio 2010, n. 78, recante misure urgenti in materia di stabilizzazione finanziaria e di competitività economica. (10G0146). Gazzetta Ufficiale n. 176 del 30 luglio 2010. Suppl. Ordinario n. 174
17. Decreto 26 febbraio 2010. Definizione delle modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al SAC. (10A03028). Gazzetta Ufficiale n. 65 del 19 marzo 2010

© SEEd Tutti i diritti riservati

18. Decreto 2 novembre 2011. De-materializzazione della ricetta medica cartacea, di cui all'articolo 11, comma 16, del decreto-legge n. 78 del 2010 (Progetto Tessera Sanitaria). Gazzetta Ufficiale n. 264 del 12 novembre 2011
19. Decreto-legge 18 ottobre 2012, n. 179. Ulteriori misure urgenti per la crescita del Paese. (12G0201). Gazzetta Ufficiale n. 245 del 19 ottobre 2012. Suppl. Ordinario n. 194
20. Decreto legislativo 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali. Gazzetta Ufficiale n. 174 del 29 luglio 2003. Suppl. Ordinario n. 123
21. Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri (FNOMCeO). Codice di deontologia medica, 2014. Disponibile online su http://www.fnomceo.it/fnomceo/Codice+di+Deontologia+Medica+2014.html?t=a&id=115184 (ultimo accesso luglio 2015)
22. Decreto 27 luglio 2005. Applicazione delle disposizioni di cui al comma 5 dell'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente i parametri tecnici per la realizzazione del software certificato che deve essere installato dalle strutture di erogazione di servizi sanitari. Gazzetta Ufficiale n. 180 del 4 agosto 2005
23. Garante per la protezione dei dati personali. Cloud computing: proteggere i dati per non cadere dalle nuvole. Disponibile online su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1895296 (ultimo accesso luglio 2015)

© SE*Ed* Tutti i diritti riservati