Gli amici di Eleonora
ONLUS

Le buone pratiche per una corretta gestione della privacy in telemedicina

Chiara Rabbito

Gli amici di Eleonora
ONLUS

Via Cervantes, 64 · 80133 NAPOLI
Tel. 081 5513233 · Fax 081 5518092
www.gliamicidieleonora.it
info@gliamicidieleonora.it

Edizione fuori commercio · Finito di stampare a Settembre 2012

Progetto grafico e stampa
Grafiche Capozzoli di Sergio Capozzoli
via Irno, località Sardone, lotto 15/17
84098 Pontecagnano Faiano · SA
tel. 089 382647 · fax 089 3856035
www.grafichecapozzoli.com · info@grafichecapozzoli.com

INDICE

INTRODUZIONE **5**

CAPITOLO PRIMO
LA PRIVACY, LA TELEMEDICINA **7**

1. La privacy 7
2. La sua evoluzione 13
3. Il regolamento dell'Unione europea 16
4. Le Linee guida per i siti web esclusivamente dedicati alla salute 21
5. La telemedicina 24
6. La sua evoluzione 29

CAPITOLO SECONDO
IL TRATTAMENTO DEL DATO SANITARIO **33**

1. Il trattamento del dato 33
2. I "protagonisti" della privacy 35
3. L'informativa e il consenso 38
4. Il dato sanitario 40
5. Quando e come il dato sanitario può essere trattato 42
6. Il consenso dell'incapace e l'emergenza sanitaria 45
7. Le modalità semplificate di rilascio dell'informativa e di raccolta del consenso 47
8. Le misure comportamentali a tutela della privacy del paziente 49
9. Le misure di sicurezza tecnica. Le misure minime di sicurezza 51
10. Le misure di sicurezza tecnica. Le misure di sicurezza idonee e preventive 54
11. La costruzione di una banca dati a contenuto sanitario 55

CAPITOLO TERZO
LA DOCUMENTAZIONE SANITARIA 59

1. Le cartelle cliniche 59
2. Il Fascicolo Sanitario Elettronico. Le Linee Guida del Garante 63
3. Il Fascicolo Sanitario Elettronico. Il riconoscimento del principio di auto-determinazione 68
4. Il Fascicolo Sanitario Elettronico. Le Linee Guida ministeriali 70
5. Il Fascicolo Sanitario Elettronico. I disegni di legge Fazio e Balduzzi ... 73
6. Il referto on line 77
7. La scheda sanitaria del medico di medicina generale 82

CAPITOLO QUARTO
BUONE PRATICHE PRIVACY PER UN PROGETTO DI TELEMEDICINA 87

1. Il progetto di telemedicina e il diritto 87
2. Il Businness Process Reengineering 90
3. La privacy: quando entra in scena? 93
4. Le buone pratiche privacy in un progetto di telemedicina 95
5. La squadra in campo: responsabili e incaricati 99
6. Il beneficiario della “macchina – privacy”: il paziente 103
7. Il percorso delle informazioni e i documenti in cui sono contenute 108
8. L’abolizione del DPS: che fare? 110

APPENDICE 115

INTRODUZIONE

La Telemedicina è ormai una tecnica indispensabile per migliorare i processi tecnologici in campo sanitario e socio-assistenziale.

Molto è stato fatto in questi anni nella sperimentazione e nella ricerca di nuovi modelli che migliorino le prestazioni e riducano i costi del servizio.

Nella maggioranza degli Ospedali italiani si usano e sperimentano cure ed assistenza con i più moderni strumenti di controllo e monitoraggio.

Diverso è l'approccio che si è utilizzato per l'assistenza domiciliare.

Scarse e, a volte empiriche, sono le sperimentazioni in corso soprattutto in settori alquanto difficili da programmare, come l'assistenza domiciliare per persone che hanno gravi patologie come il coma o gli stati vegetativi permanenti.

Grazie all'intervento finanziario della Fondazione con il Sud noi abbiamo attivato un progetto sperimentale unico nel suo genere.

Infatti la telemedecina non viene utilizzata solamente per controllare a distanza e monitorare i comportamenti di malati gravi come le persone in S.V., ma abbiamo inserito nel novero delle informazioni da raccogliere e monitorare anche i comportamenti sociali della famiglia.

Nell'equipe socio-assistenziale sono presenti psicologi, clown dottori, sociologi.

In una parola il *care giver*, la famiglia viene assistita e se occorre curata.

Fondamentale per la riuscita del progetto e la salvaguardia dei dati è il rispetto della privacy.

Per questo abbiamo studiato, insieme con l'Avv. Chiara Rabbito, tutti gli aspetti da valutare, applicando un rigido protocollo.

Questa pubblicazione è il primo lavoro prodotto nell'ambito del progetto.

Lo mettiamo a disposizione della comunità scientifica, con la speranza che possa essere utile ad operatori e familiari.

È un percorso lungo quello che ci attende, ma siamo convinti che è solo la ricerca che può dare risposte positive ed innovative alle tante incognite che si trovano ad affrontare le persone in S.V., ma soprattutto chi le deve curare o assistere.

Claudio Lunghini
Segretario Onlus Gli Amici di Eleonora

CAPITOLO PRIMO

LA PRIVACY, LA TELEMEDICINA

1. La privacy

Quando scrivo di privacy, specie se si tratta di privacy applicata alle nuove tecnologie, sono consapevole di rivolgermi ad un pubblico di lettori ondeggiante tra la diffidenza circa la reale utilità di quanto sto per trattare e il senso di smarrimento e di timore per un tema articolato e percepito spesso come oscuro nelle sue molteplici implicazioni.

Un aneddoto che ogni tanto mi piace raccontare ai convegni per introdurre la privacy in un clima di – potrei dire – maggior rilassatezza è quello, assai noto, circa le origini del *right to privacy* (del diritto alla privacy, diremmo noi).

Un episodio che, non solo ci aiuta a leggere la privacy come una questione meno distante e astrusa di quanto non ci sembri, ma che - a mio giudizio - illumina quella che dovrebbe essere la caratteristica essenziale della privacy, chiave di comprensione e di interpretazione della molteplicità delle norme e delle regole che la riguardano: il fatto di essere, in fin dei conti, una faccenda *molto personale*, o meglio, come diremmo noi giuristi, un *diritto a tutela della personalità* dell'individuo[1], e cioè tra i più importanti che gli ordinamenti giuridici riconoscano e che le norme costituzionali proteggano.

Ora il fatto (come vi accennavo, molto raccontato) è questo: i primi a scrivere di privacy, anzi ad avanzare l'ipotesi, per l'epoca estremamente nuova, dell'esistenza di un "diritto alla privacy" (*the right to privacy*, appunto) furono due avvo-

[1] I diritti della personalità fanno riferimento a situazioni giuridiche soggettive che tutelano l'identità, la vita, l'integrità fisica, la dignità e la reputazione di ciascun essere umano. Sono diritti riconosciuti a tutti gli esseri umani indistintamente e che sorgono al momento stesso della nascita dell'individuo. La persona cui fanno capo non se ne può spogliare in nessun caso.

Nel caso del diritto della privacy, in Italia tale diritto non è previsto espressamente da una norma costituzionale, tuttavia non se ne mette in dubbio la tutela di livello costituzionale in quanto essa è ricavabile per via interpretativa dal complesso di norme che proteggono le differenti manifestazioni esterne di tale diritto: inviolabilità del domicilio, libertà e segretezza di ogni forma di comunicazione, pari dignità sociale dei cittadini, tutela del nome e dell'immagine.

cati statunitensi, Louis Brandeis e Samuel Warren, che affrontarono la questione in un articolo pubblicato nella prestigiosa Harvard Law Review nel 1890[2].

La loro visione della privacy, quella che poi per molto tempo fu l'unica, voleva l'affermazione di un diritto delle persone *"to be let alone"*.

La traduzione letterale che ne faremmo noi italiani non rende granché. Non si trattava infatti tanto del diritto a "essere lasciati soli" quanto piuttosto del diritto ad essere "lasciati in pace", del diritto alla intimità della propria vita privata, del diritto a che gli altri cittadini, la stampa, le istituzioni (a meno che non fosse necessario e previsto dalla legge), si astenessero dal ficcare il loro naso curioso nelle nostre sacrosantamente private faccende.

La privacy, dunque, come vi dicevo, è prima di tutto una faccenda *molto personale*.

Quel che si racconta è poi ancora più utile per darci un'idea di quanto fosse "personale" l'origine della elaborazione del diritto alla privacy.

I dotti sottolineano come Brandeis sia stato ispirato dalla lettura dell'opera di Ralph Wald Emerson, filosofo statunitense che proponeva la solitudine come criterio e fonte di libertà.

Ma, si racconta anche, tra una riflessione dotta e l'altra, che Warren, l'altro autore dell'articolo, avvocato a Boston, fosse parecchio – potremmo dire - urtato dal comportamento della stampa poco rispettoso e più teso alla vendita dei giornali che non alla ricerca della verità.

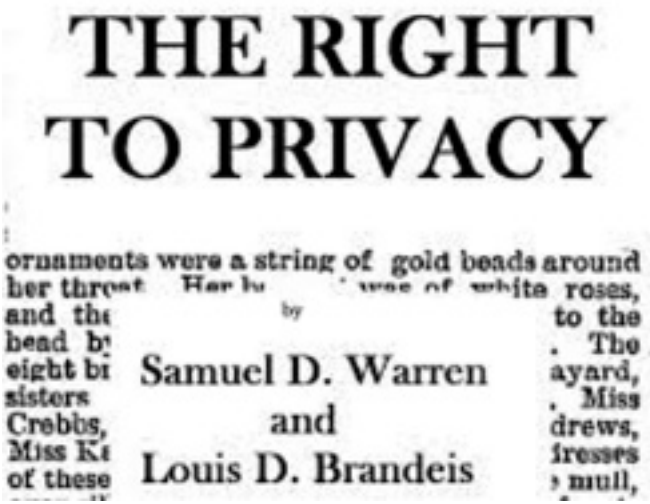
Siamo agli esordi del fotogiornalismo e i giornali, prodighi di foto e zeppi di articoli per quei tempi scandalistici, tenevano sotto la loro lente d'ingrandimento la vita privata dell'avvocato Warren, la sua famiglia e in particolare sua moglie.

Il suo matrimonio con la figlia di un senatore, fin dal suo annuncio, era stato costantemente sotto i riflettori della stampa; le vicende della famiglia, le amicizie della moglie, persino i loro acquisti più costosi, venivano esposti continuamente dai giornali alla pubblica pruriginosa (così egli si esprime) curiosità.

Il fatto fece venire la mosca al naso a Warren, che - da buon avvocato -, rispose, insieme all'amico, ex compagno di università e collega di studio, Brandeis, con un bell'articolo giuridico sulla elaborazione concettuale del diritto alla

[2] L. Brandeis, S. Warren, *The Right to Privacy*, Harward Law Review, 1890.

privacy, il primo nella storia del diritto. Con buona pace di chi, con evidentemente differente approccio, i giornalisti "semplicemente" li querela.


THE RIGHT
TO PRIVACY

ornaments were a string of gold beads around
her throat. Her hu ' was of white roses,
and the by to the
head b . The
eight bi Samuel D. Warren ayard,
sisters . Miss
Crebbs, and drews,
Miss Ka Louis D. Brandeis fresses
of these mull,

L'individuazione del diritto alla privacy ha dunque a che fare con un episodio molto privato e anche con quel pizzico di mondanità che ci aiuta ad affrontarlo con un po' meno di timore reverenziale, giustissimo, per carità, purché non sia paralizzante.

E come una questione innanzitutto privata, e che tocca da vicino i nostri fondamentali diritti di persone, ritengo vada ancor oggi letta.

Col tempo, le cose si sono, lo sappiamo, un po' complicate. Intanto per via del buon Rousseau, che non lo si poteva trascurare[3].

[3] Jean-Jacques Rousseau (1712-1778) filosofo svizzero illuminista nella sua opera *Il Contratto sociale (Du contrat social: ou principes du droit politique)*, pubblicato nel 1762, scrive della necessità per l'individuo che intende organizzarsi in una società di "trovare una forma di associazione che difenda e protegga, mediante tutta la forza comune, la persona e i beni di ciascun associato e per mezzo della quale ognuno, unendosi a tutti, non obbedisca tuttavia che a se stesso e rimanga libero come prima". A giudizio di Rousseau, grande precursore delle idee politiche moderne, l'unica forma di associazione che risponde a ciò è lo Stato democratico, che consente al cittadino di conservare la propria libertà e uguaglianza, in quanto in uno Stato democratico il popolo è il Sovrano e tale Stato esercita (o dovrebbe esercitare) la volontà generale dei cittadini.

Se è vero infatti che possiamo e dobbiamo rivendicare in molte situazioni il nostro diritto alla privacy, è vero anche che non siamo pionieri isolati che nel selvaggio West difendono il proprio spazio a colpi di fucile.

Siamo, volenti o nolenti, membri di una società, cittadini di uno Stato, del cui buon governo, del cui ordine e della cui sicurezza dobbiamo preoccuparci e con cui dobbiamo, per il bene di tutti, collaborare.

Insomma, il patto sociale, a tutti i livelli, va onorato. Questo comporta dei limiti, come si può facilmente immaginare, al nostro buon diritto di essere lasciati pace.

Il diritto alla privacy, come del resto molti diritti della personalità costituzionalmente tutelati, si è dunque dovuto contemperare a superiori esigenze, lo si è dovuto regolamentare, dirigere, limitare per il buon funzionamento dello Stato e per la corretta convivenza con gli altri individui.

Si è cominciato a parlare di "diritto alla riservatezza", il cui contenuto individua le regole in base alle quali i nostri dati devono essere correttamente e lecitamente trattati.

Non si è pertanto più mirato ad escludere gli altri dall'impiego dei nostri dati, quanto piuttosto ad elaborare i principi, i criteri, le regole di un lecito trattamento dei dati personali.

E qui nasce il primo genere di problemi: la individuazione e la corretta comprensione delle modalità e dei limiti di un tale trattamento affinché possa definirsi "lecito", in tutte le possibili articolazioni, situazioni, graduazioni, sfumature.

Questa è la prima sfida, impegnativa, continua, spesso faticosa: quando il trattamento di un dato personale è lecito? Quando prevale il diritto primario dell'individuo a che i suoi dati non siamo "toccati" e quando invece interessi più importanti lo rendono necessario? Qual è il corretto bilanciamento tra la privacy e gli altri diritti tutti egualmente tutelati a livello costituzionale, quali la salute, l'ordine e la sicurezza pubblica, il diritto di cronaca, la libertà d'impresa, e molti altri potremmo citarne. Quando prevale l'uno e quando un degli altri ugualmente rilevanti?

Poi è arrivato Internet, sono arrivate le tecnologie informatico- telematiche, che sono state origine di tutta una serie di altri problemi in materia di privacy, e di conseguenza, di una nuova visione di essa.

Non si è trattato semplicemente della necessità di tener conto della rivoluzione informatica (e quindi del fatto che progressivamente le informazioni venivano espresse nel nuovo formato digitale, che le rendeva più facilmente copiabili e duplicabili, oltre che massicciamente conservabili nei nuovi archivi elettronici o database), ma si trattava di adeguare la lettura del diritto alla riservatezza ad un mondo - quello della società dell'informazione telematica - in cui l'informazione può essere fatta "viaggiare" attraverso la rete con estrema rapidità, senza particolari difficoltà tecniche e in modo facilmente non controllato.

Quindi ecco che si tratta di affrontare una nuova ulteriore sfida: ripensare il diritto alla privacy calandolo in un mondo fatto di enormi quantità di informazioni che possono essere facilmente e rapidamente spostate grazie al web, spesso senza preordinati controlli e con illimitate possibilità di duplicazione e di archiviazione.

A questo scenario si aggiunga una pericolosa tendenza alla mercificazione delle informazioni, che stoccate in grandissime quantità e organizzate secondo adeguati criteri di ricerca, possono divenire appetibile oggetto di acquisto per i più svariati fini tendenti al privato lucro.

Un panorama dunque complesso, pericoloso, in rapidissima evoluzione, che ha reso necessaria una legislazione in materia di privacy anch'essa abbondante, articolata, complessa e - secondo alcuni - addirittura ipertrofica.

L'obiettivo della produzione normativa in materia di privacy (italiana, europea, mondiale) è tuttavia comprensibile e immediato: non più il nostro diritto ad essere lasciati soli ma anzi il nostro diritto a non essere abbandonati a un universo di pirati informatici, ad una giungla selvaggia e sregolata popolata di "mostri telematici", che strumentalizzano ai loro fini - non leciti - le informazioni su di noi, la nostra identità digitale, la nostra storia, le nostre più private faccende.

L'informatica combinata alla telematica, la possibilità di trattare enormi quantità di dati a velocità elevatissime, hanno infatti reso concretamente possibile il nostro peggiore incubo in materia di privacy: la possibilità di "pescare" nel web, raffrontare, combinare e assemblare i nostri dati personali della più varia provenienza, arrivando così a tracciare profili dettagliati di noi stessi, seguendoci in ogni nostra attività e in ogni nostra espressione.

Il pericolo insito nei trattamenti informatizzati risiede proprio nella possibilità di combinare tra loro i dati personali di un soggetto che, in sé considerati, sarebbero poco significanti, fino a costituirne un complesso organico, da cui risulterà possibile trarre indicazioni su quell'individuo particolarmente espressive e a vari fini, non necessariamente leciti.

Un bagaglio di notizie su di noi, la nostra famiglia, i nostri cari suscettibile di essere – ahimé - venduto e comprato da personaggi non raccomandabili per denaro e per i più svariati motivi, in genere collegati al commercio: spiare i nostri gusti o le nostre necessità per venderci un prodotto, sapere se siamo buoni clienti per un'assicurazione sulla vita, verificare se faremo fronte al finanziamento richiesto, scoprire se siamo sensibili ad una o ad un'altra causa benefica per una certa tale raccolta fondi, e via così : tutto ciò che può venire in mente a truffatori ben informati.

Da tutto questo, dal furto della nostra identità digitale, ma direi anche della nostra "personalità digitale", dei nostri gusti, delle nostre abitudini e delle nostre aspirazioni affidate alla rete, la nuova concezione della tutela della privacy mira a proteggerci, tanto più e tanto più fortemente se i dati trattati afferiscono alla nostra sfera più intima: alle nostre convinzioni ideologiche, politiche, religiose, e ancora a maggior ragione, al nostro stato di salute.

Pensate quali e quanti danni può fare una mercificazione bieca e senza scrupoli delle notizie sul nostro stato di salute, qualora esse fossero reperibili sul web senza filtri e senza un debito controllo.

Senza contare che l'ambito "salute" afferisce ad una sfera così personale e intima dell'individuo che le informazioni che la riguardano vanno tutelate sempre e comunque, per rispetto alla persona, alla sua dignità, al suo diritto – in questo caso sì - di essere "lasciato solo", qualora egli ne senta la necessità, solo con sé stesso o solo con i propri cari, affinché quanto riguarda il suo stato di salute non sia scriteriatamente abbandonato alla pubblica curiosità, sia essa quella del vicino di casa o degli internauti che popolano il web.

La legislazione italiana che tutela i nostri dati sanitari probabilmente è lontana da livelli di assoluta completezza e perfezione che ci potremmo augurare, ma sicuramente un merito al nostro legislatore va riconosciuto: quello di puntare fortemente, con molti dei mezzi possibili, sia nel mondo reale e

che nel mondo virtuale, alla maggior tutela possibile dell'individuo e della sua dignità.

La *ratio legis*, come la chiamano i giuristi, la motivazione che anima le nostre norme in materia di trattamento del dato sanitario è incentrata nel riconoscimento del valore e della dignità della persona, non del malato, ma della persona in tutta la sua pienezza e libertà.

E lo dimostra il fatto che la tutela si estenda a tutti i dati attinenti alla salute, non ai soli dati che riguardano eventuali patologie, che essa si applichi anche qualora, per intenderci, l'informazione da tutelare fosse: "non ci sono patologie".

Come dire: i dati dell'individuo, la sua privacy, vanni tutelati sempre e in ogni caso, vi siano patologie in corso o no, sia la persona malata o sana, normodotata o diversamente abile. Quello che importa è la persona, non la sua condizione.

Questo principio a mio giudizio - bisogna darne atto al nostro legislatore - emerge fortemente dalla nostra normativa a tutela della privacy.

2. La sua evoluzione

Il diritto alla riservatezza riceve quindi una sua prima formulazione nell'articolo di Brandeis e Warren che, argomentando correttamente sulla base del fatto che "I mutamenti politici e sociali obbligano al riconoscimento di nuovi diritti", di fronte al massiccio diffondersi della carta stampata e all'uso spesso distorto che ne viene fatto invocano il diritto dell'individuo a "essere lasciato solo".

E questa è la lettura che principalmente si darà del diritto alla privacy fino alla metà del Novecento.

È evidente come nella società attuale tale accezione della privacy non potesse bastare.

Sebbene la qualificazione di essa quale diritto di livello costituzionale fosse ancora da venire, se ne trova una importante menzione nella Convenzione dei diritti dell'Uomo del 1950, il cui art. 8 afferma che: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza".

Tale affermazione verrà ripresa nella Carta dei diritti fondamentali dell'Unione europea, che fu proclamata ufficialmente a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione.

Nel dicembre 2009, con l'entrata in vigore del trattato di Lisbona, è stato conferito alla Carta lo stesso effetto giuridico vincolante dei trattati, cioè impegna gli Stati che lo abbiano ratificato[4].

L'articolo 7, rubricato "Rispetto della vita privata e della vita familiare" ribadisce "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni". Più dettagliatamente l'art. 8 della stessa Carta, dal titolo "Protezione dei dati di carattere personale" recita: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o un altro fondamento legittimo previsto dalla legge. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'Autorità indipendente".

In piena coerenza con il principio espresso nella Convenzione dei diritti dell'Uomo, venne emanata nel 1995 la Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

Come noto, nel diritto dell'Unione europea la direttiva è uno degli atti che il Parlamento congiuntamente con il Consiglio può adottare per l'assolvimento dei compiti previsti dai trattati, perseguendo un obiettivo di armonizzazione delle normative degli Stati membri.

[4] Il trattato è una delle principali fonti del diritto internazionale e consiste nell'incontro delle volontà di due o più Stati diretti a disciplinare rapporti intercorrenti tra essi. Un trattato internazionale, essendo un accordo che vincola due o più parti e avendo quindi natura negoziale, presenta molti profili comuni a gran parte delle discipline contrattuali dei vari diritti interni. Ciascuno Stato, attraverso suoi rappresentati, detti plenipotenziari, adotta un testo comune e provvede a firmarlo. La firma del testo votato *non ha valore vincolante per gli Stati*. Ciascuno Stato si impegna invece ad osservare il trattato attraverso la cosiddetta *ratifica*, che è atto che ha meccanismi diversi da nazione a nazione ed è previsto nella costituzione di ciascuna.

È così previsto normativamente: "La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi[5]".

La direttiva detta quindi agli Stati membri un obbligo di risultato: lo Stato deve garantire l'effetto voluto dall'Unione. Allo Stato è inoltre posto un obbligo di *stand still*: cioè nel periodo antecedente il termine di attuazione non può adottare atti in contrasto con gli obiettivi della direttiva.

In fase di recepimento, la nazione che attua la direttiva deve comunicare la forma e i mezzi attraverso i quali la direttiva è stata recepita sì da permettere, nel caso, alla Corte di giustizia dell'Unione europea di valutare se i mezzi adottati corrispondono al principio di certezza del diritto.

A seguito della emanazione della direttiva sulla privacy, lo Stato italiano si trovava dunque vincolato, per la sua stessa natura giuridica di membro dell'Unione (all'epoca Comunità Europea), al suo recepimento. Cosa che avvenne mediante la legge 31 dicembre 1996 del 675.

La prima legge sulla privacy è stata quindi introdotta in Italia su impulso del legislatore europeo e, in conformità ai principi contenuti nella direttiva, essa si prefiggeva di tutelare tutti i consociati, e non più solo le persone "note", e di proteggere i cittadini non meramente da un'invasione nella loro sfera privata ma nei confronti di ogni possibile abuso perpetrabile attraverso il trattamento dei loro dati personali.

Alla legge 675 seguì poi il Codice della privacy, contenuto nel d.lgs. 30 giugno 2003, n. 196.

Si apre così una nuova fase della tutela del diritto alla riservatezza nel nostro ordinamento, rispondendo il nuovo Codice all'esigenza, da tempo avvertita, di un unico testo legislativo, in grado di coordinare e integrare le numerose disposizioni normative e regolamentari succedutesi nel breve lasso di tempo trascorso dall'emanazione della legge 675.

[5] Art. 288 TFUE – Trattato sul funzionamento dell'Unione Europea, 3° comma.

3. Il regolamento dell'Unione europea

L'Unione europea è ora in via di adozione di un nuovo complesso di norme a tutela della privacy. Sarà principalmente un regolamento comunitario a dettarne la disciplina.

La precedente regolamentazione, tuttora vigente, era contenuta - come si è detto - nella direttiva 95/46/CE[6].

Il nuovo strumento scelto dal legislatore europeo per normare la privacy, il regolamento appunto, ha caratteristiche completamente diverse rispetto alla citata direttiva.

La direttiva, come si è detto, è un atto del legislatore dell'Unione europea che vincola i singoli Stati membri *solo* con riguardo ai risultati da conseguire. Il *come* quei risultati saranno conseguiti è compito dei singoli Stati stabilirlo.

La direttiva, quindi, stabilisce i principi. Ciascun legislatore interno decide come dettagliare quei principi nelle norme di recepimento della direttiva (nel caso italiano le direttive comunitarie vengono in genere recepite con legge o mediante decreto legislativo).

Conseguenza ne è che la materia presa in considerazione da una determinata direttiva e di cui quella direttiva stabilisce i criteri fondamentali di regolamentazione, sarà poi di fatto normata in modo differente da Stato a Stato, in base al grado di discrezionalità lasciato dal legislatore comunitario ai singoli legislatori interni.

Vi potranno essere differenze più o meno forti, ma il recepimento di una direttiva comporterà sempre una regolamentazione differente – in modo più o meno rilevante – da Stato a Stato.

Nel caso della emanazione di un regolamento la situazione è completamente diversa.

Il regolamento è *direttamente applicabile* all'interno di ciascuno Stato membro: «Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri»[7].

I regolamenti comunitari, quindi, a differenza delle direttive, non necessitano di alcun atto di recepimento o di attuazione, che sarebbe superfluo e anzi incompatibile. Vengono perciò definiti: *"self-executing"*.

[6] Direttiva del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

[7] Art. 288 comma 2 TFUE.

Il processo di riorganizzazione della normativa privacy è partito il 25 gennaio di quest'anno, quando la Commissione europea, preso atto che il progresso tecnologico e la globalizzazione hanno profondamente modificato il modo in cui i dati sono raccolti, utilizzati e attraverso cui vi si accede, ha proposto una riforma complessiva delle regole di protezione dei dati contenute nella direttiva del '95 al fine di rafforzare i diritti della privacy on line e di promuovere lo sviluppo dell'economia digitale europea[8]

La Commissione europea ha anche constatato come i ventisette Stati membri dell'Unione abbiano attuato differentemente la direttiva europea del 1995, con conseguenti nette disuguaglianze sotto il profilo delle applicazioni concrete delle norme.

Ad avviso della Commissione, si rende necessaria una legge singola per tutti i ventisette Stati europei, al fine di eliminare l'attuale frammentazione normativa e i costosi aggravi amministrativi, con un risparmio per le imprese calcolato in circa 2,3 miliardi di euro all'anno.

Il legislatore comunitario si prefigge quindi di dettare una normativa, unica per tutta l'Europa, che proteggendo scrupolosamente i dati personali dei cittadini nel mondo digitale, rafforzi la fiducia dei consumatori nei servizi on line, consentendo la necessaria crescita economica e l'indispensabile sviluppo del lavoro e dell'innovazione[9].

Le differenze nel livello di protezione dei dati personali in base al luogo in cui una persona vive o compra dei beni o dei servizi sono quindi dannose secondo la Commissione europea e producono come conseguenza una generale diffidenza da parte dei consumatori dei servizi on line, che non si sentono adeguatamente tutelati.

[8] Citando letteralmente: "Brussels, 25 January 2012 – The European Commission has today proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used". Nel sito dell'Unione europea, al link: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[9] "A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe".

Poiché Internet e il mondo digitale generano e hanno vita nella globalizzazione, allora le norme che li regolamentano devono essere quanto più possibile globali.

Quali saranno i principi cardine della nuova regolamentazione dei dati personali nel mondo digitale?

Innanzitutto, ci dice la Commissione, un rafforzamento del diritto all'oblio, cioè del diritto ad essere "dimenticati dalla rete": dovrà essere *sempre* possibile chiedere la cancellazione dei proprio dati se non vi è motivo legittimo per la loro conservazione.

Inoltre ci si prefigge un rafforzamento del valore dell'atto del consenso: il consenso, quando necessario per il trattamento del dato, dovrà sempre essere *dato esplicitamente*, *non potrà mai essere supposto*.

Con riguardo all'obiettivo di uniformazione della regolamentazione e della tutela, si prevede che le organizzazioni titolari dei dati (aziende, pubbliche amministrazioni, associazioni) dovranno rapportarsi ad un'unica autorità garante nazionale di protezione dei dati: quella del paese dell'Unione in cui hanno la propria sede principale.

La norma, giustamente, si prefigge di mettere ordine nelle possibili situazioni di confusione e disorientamento causate dalla internazionalità, dalla – meglio – globalità del mondo digitale. Come sappiamo molte aziende che forniscono servizi digitali (e che quindi sono presenti in rete) hanno molte sedi, una sede legale, una o più sedi operative, molte succursali in diversi paesi. Sono inoltre virtualmente presenti in molti paesi attraverso i loro siti internet e, poiché forniscono servizi mediante la rete, operano on line in moltissimi paesi, quindi hanno partner, clienti, consumatori appartenenti a molti diversi Stati dell'Unione europea (e anche non appartenenti a questa).

Nel caso in cui ci siano problemi con riguardo alla tutela dei dati personali quale sarà l'Autorità garante che dovrà controllarli? Sarà, ci dice la Commissione europea, una sola e, in particolare, quella dello Stato membro in cui hanno la loro sede principale[10].

[10] Si deve precisare che, con approccio correttamente pratico e finalizzato a smascherare raggiri burocratici, la sede principale di un'azienda non è, per il legislatore comunitario, la sua sede legale, ma quella in cui viene svolta principalmente la sua attività e in cui sono principalmente situati i suoi interessi.

Ma dal lato del consumatore come ci si comporterà? Il consumatore, disorientato dalla pluripresenza e internazionalità di un fornitore di servizi digitali che sta danneggiando i suoi diritti di protezione dei dati on line, a chi si dovrà rivolgere? Dovrà sforzarsi di individuare qual è la sede principale del truffatore e chiamare in aiuto l'Autorità garante di quel (magari lontano) Paese?

A massima tutela del consumatore, non sarà così: il legislatore comunitario ha stabilito che in caso di violazione della tutela dei propri dati da parte di un'organizzazione, sarà possibile rivolgersi all'autorità di protezione dei dati del *proprio* paese, *anche se i dati sono trattati da un'impresa con sede fuori dell'Unione*.

Viene quindi introdotto il principio dell'applicazione del diritto comunitario anche ai trattamenti di dati personali non svolti nell'Unione europea, se relativi all'offerta di beni o servizi a cittadini dell'Unione o tali da consentire il monitoraggio dei comportamenti di cittadini UE.

Sulla base di quanto detto, potrà anche verificarsi che un'Autorità garante nazionale si trovi ad applicare il regolamento rispetto a un trattamento dei dati personali che riguarda cittadini di altri paesi dell'Unione, oppure a prendere decisioni che coinvolgano cittadini di altri paesi.

Per questi casi viene introdotto il meccanismo cosiddetto del *one stop shop*: l'Autorità garante coinvolta sarà tenuta a chiedere il parere del gruppo del Garanti europei[11] e a lavorare insieme ad almeno altre due Autorità.

L'obiettivo che ci si prefigge è quello di uniformare il più possibile tra tutti i paesi membri non solo la legge privacy di riferimento, ma anche il modo in cui essa viene interpretata e applicata dalle singole Autorità garanti, in modo che per le imprese e per i cittadini non sia più possibile, come invece oggi accade, scegliere tra tutti quelli dell'Unione il paese più "normativamente compiacente" per effettuare un trattamento dei dati: tutte le Autorità saranno sottoposte a regolazione uniforme e dovranno operare in coordinamento per assicurare l'omogeneità nel trattamento dei dati, la legge sarà la stessa su

[11] Il Working Group Art. 29 prenderà il nome di "Consiglio Europeo per la Protezione dei Dati personali".

tutto il territorio europeo e quindi diminuirà la discrezionalità delle singole autorità nazionali.

Con riguardo all'utilizzo delle tecnologie informatiche e telematiche, viene introdotto un requisito di legittimità di queste che prevede una operazione cosiddetta di *privacy impact assessment*, cioè sarà necessaria una previa valutazione dell'impatto-privacy.

In sede di progettazione di un prodotto o di un software sarà necessaria una contestuale previsione delle misure di sicurezza da applicare (cosiddetta *privacy by design*), come a dire che il software non deve essere prima progettato e poi ne devono essere pensate le misure a tutela della privacy, ma che il software deve nascere ed essere sviluppato insieme alle cautele della privacy, che ne saranno parte integrante.

Le sanzioni previste in caso di violazione saranno molto alte e potranno arrivare fino al 2% del volume d'affari annuale mondiale di un'impresa.

Come si è detto il nuovo regolamento sarà direttamente applicabile all'interno di ciascuno Stato membro. Ne conseguirà un forte impatto sui singoli Codici privacy nazionali, in quanto non potranno essere più applicate le norme che risulteranno incompatibili con il regolamento.

La difficoltà degli interpreti e delle corti nazionali sarà di volta in volta appurare quali siano le norme interne che devono essere considerate "incompatibili" con il regolamento.

L'iter legislativo per l'approvazione definitiva sarà comunque piuttosto lungo, in quanto esso richiede l'approvazione congiunta del Parlamento europeo e del Consiglio nella procedura di co-decisione[12]: si prevede che ci vorrà circa un anno dalla presentazione della proposta per arrivare a conclusione.

Circa poi i tempi di applicazione, anch'essi sono piuttosto dilatati, in quanto l'applicazione dovrà avvenire entro due anni dall'entrata in vigore: si tratta, quindi nel complesso, di un periodo di tre anni per arrivare alla "messa a regime" del regolamento.

[12] Ora definita dal Trattato di Lisbona "procedura legislativa".

La Commissione Europea

4. Le Linee guida per i siti web esclusivamente dedicati alla salute

Lo stesso giorno, il 25 gennaio del 2012, in cui la Commissione europea ha presentato la sua proposta di regolamento, il Garante italiano ha deliberato di adottare le "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute"[13], linee guida cui vale la pena di fare un cenno per l'attinenza della materia disciplinata a questa nostra trattazione.

Il Garante, nelle premesse, dice di aver constatato come sempre più spesso si faccia ricorso alle potenzialità di Internet anche per discutere e approfondire le tematiche inerenti alla salute, sia da parte dei medici, che in questo modo si scambiano informazioni e pareri e condividono esperienze scientifiche e umane, sia da parte degli utenti non medici.

L'Autorità, pur riconoscendo l'utilità di questo scambio in rete di conoscenze scientifiche e di esperienze umane e l'importanza della creazione, attraverso il

[13] Provvedimento n. 31 del 25 gennaio 2012, pubblicato sulla Gazzetta Ufficiale n. 42 del 20 febbraio 2012.

web, di reti di solidarietà e di sostegno tra gli utenti/pazienti, mette tuttavia in guardia sulla pericolosità di questo scambio di informazioni se effettuato con modalità non protette: "il trattamento nella rete di dati sensibili e, in particolare, dei dati che riguardano la salute degli utenti presenta profili di rischio per i diritti e le libertà fondamentali, nonché per la dignità dei soggetti interessati, in relazione alla particolare delicatezza dei dati trattati e delle caratteristiche di Internet".

Allo scopo, pertanto, di conseguire una maggiore sensibilizzazione e attenzione agli aspetti che riguardano il corretto trattamento dei dati personali e sensibili, ha adottato le citate Linee guida.

Esse si prefiggono di fornire indicazioni e raccomandazioni atte a "prevenire i rischi connessi alla pubblicazione e diffusione dei dati relativi alla salute in Internet e, in particolare, ad evitare un'impropria esposizione delle persone e dei loro dati più intimi nella rete" e di rendere gli utenti maggiormente consapevoli dei pericoli per la loro privacy.

Le raccomandazioni contenute nelle Linee guida sono rivolte ai gestori dei siti web dedicati esclusivamente alla salute (specifici forum e blog, specifiche sezioni di portali che contengono informazioni sanitarie, nonché social network che si occupano di tematiche sulla salute), nei quali si svolge un'attività di carattere meramente *divulgativo e conoscitivo*, non solo con riferimento alle informazioni e ai commenti che si scambiano gli utenti, ma anche con riferimento ai consigli o alle "consulenze" mediche che vengono dagli stessi richieste.

Pertanto, non rientrano nell'ambito considerato dalle linee-guida i servizi di assistenza sanitaria on line e la telemedicina che, con riguardo alla cura della salute, si inquadrano invece nella prestazione medica in senso stretto.

Nell'ambito dei siti web dedicati esclusivamente alla salute, il Garante distingue i siti che prevedono la registrazione dell'utente per partecipare alle relative attività e siti che non prevedono tale registrazione.

Ai gestori di siti web sulla salute che prevedono la registrazione dell'utente per l'accesso al sito e alle sue prestazioni, il Garante raccomanda di fornire l'informativa prima della compilazione del modulo di raccolta dei dati di registrazione e invitare l'utente a confermare, apponendo un segno di spunta in un'apposita casella, l'avvenuta presa visione dell'informativa; indicare le

finalità per le quali i dati sono raccolti e le modalità del relativo trattamento; specificare quali dati di registrazione sono ritenuti necessari per partecipare alle attività del sito e quali dati sono invece ritenuti facoltativi; indicare i tempi di conservazione dei dati personali raccolti; indicare i diritti dell'interessato di cui all'art. 7 del Codice; rendere sempre visibili e facilmente reperibili i propri estremi identificativi di titolare del trattamento, o quelli del responsabile, cui sia possibile chiedere riscontro in relazione ai diritti di cui all'art. 7 del Codice.

Con riguardo ai summenzionati diritti si sottolinea che l'interessato ha sempre il diritto, qualora non intenda più partecipare alle attività del sito (forum, blog etc.), di ottenere *la cancellazione dei propri dati personali*; analogamente, può richiedere l'aggiornamento, la rettificazione ovvero l'integrazione dei dati stessi. A tal fine l'interessato può rivolgere un'apposita richiesta al gestore del sito, in quanto titolare del trattamento, secondo le modalità previste dal Codice.

In considerazione della particolare delicatezza dei dati personali che vengono trattati, al gestore è richiesto di rendere anche una specifica *"avvertenza di rischio"*, volta a richiamare l'attenzione dell'utente, segnalandogli il pericolo che, *immettendo dati sensibili collegati a dati identificativi nel sito web, si può essere individuati con la propria specifica patologia*.

Nella avvertenza di rischio il Garante raccomanda al gestore di:

- specificare che, qualora l'utente desideri mantenere l'anonimato, è possibile non inserire il proprio nome e cognome, utilizzando, invece un *nickname*;
- specificare che i dati di contatto (quali ad esempio l'indirizzo di posta elettronica), da fornire all'atto della registrazione al sito, non verranno automaticamente pubblicati sul sito insieme ai commenti dell'utente;
- avvertire l'utente di valutare con la necessaria attenzione l'opportunità, nei propri interventi, di inserire, o meno, dati personali – compreso l'indirizzo e-mail- che possano rivelarne, anche indirettamente, l'identità [14];
- avvertire l'utente di valutare l'opportunità o meno di pubblicare foto o video che consentano di identificare o rendere identificabili persone e luoghi;

[14] Si pensi, ad esempio, al caso in cui in cui l'utente, nel testimoniare la propria esperienza o descrivere il proprio stato di salute, inserisca riferimenti a luoghi, persone, circostanze e contesti che consentano anche indirettamente di risalire alla sua identità.

- avvertire l'utente di prestare particolare attenzione alla possibilità di inserire, nei propri interventi, dati che possano rivelare, anche indirettamente, l'identità di terzi, quali, ad esempio, altre persone accomunate all'autore del post dalla medesima patologia, esperienza umana o percorso medico;
- specificare l'ambito di conoscibilità dei dati propri o altrui, precisando se tali dati siano consultabili soltanto dagli iscritti al sito, ovvero da qualsiasi utente che acceda al sito stesso;
- precisare se i dati sono indicizzati e reperibili o meno anche dai motori di ricerca generalisti (Google, Yahoo etc.).

I dati raccolti dal gestore del sito su sua richiesta devono inoltre essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta[15]. Naturalmente i dati raccolti dal gestore devono restare riservati (ivi compreso l'indirizzo e-mail) e non possono essere comunicati o diffusi a terzi.

Nel caso in cui il servizio sia realizzato mediante il sito web con un'organizzazione o di un'azienda (ad esempio un editore), il gestore dovrà garantire che i dati dell'utente non siano utilizzati da personale non autorizzato e per finalità che non sono conformi alla volontà espressa o implicita dell'utente stesso.

Per quanto concerne i siti web che *non* prevedono la registrazione dell'utente, ai gestori non è richiesto di rilasciare l'informativa, in quanto non vi è trattamento di dati personali di registrazione. L'utente però inserisce informazioni che lo riguardano – anche relative alla sua salute - negli spazi dedicati del sito, quindi il Garante richiede comunque al gestore di fornirgli l'avvertenza di rischio, con le medesime caratteristiche di quella prevista per i siti con registrazione.

5. La telemedicina

Le origini della telemedicina sono relativamente recenti se le si considera in rapporto alla storia dell'uomo, ma già piuttosto datate a vederle nell'ottica della "storia delle nuove tecnologie".

[15] Art. 31 e seguenti del Codice.

Esse si fanno risalire agli anni Sessanta - Settanta del Novecento e i primi a sperimentare l'applicazione delle tecnologie informatiche e telematiche alla medicina sarebbero stati gli Statunitensi, spinti dalla necessità di studiare un modo per prestare assistenza medica – o svolgere normale attività di monitoraggio delle funzioni vitali – agli astronauti impegnati nelle prime, storiche missioni spaziali.

Essi definirono *"e-Health"* l'insieme di queste nuove applicazioni informatico-telematiche e ne intesero il risultato come "l'assistenza medica prestata a pazienti lontani mediante i mezzi di telecomunicazione e l'informatica".

I termini impiegati per indicarle sono stati nel tempo molteplici: non solo *e-Health*, ma anche *digital Healthcare* e *informatics Health*[16] – tradotta nell'italiano "informatica sanitaria", telemedicina (dal francese *telemedicine* impiegato dal legislatore europeo), per arrivare alle espressioni italiane di *sanità elettronica* e *medicina telematica*.

Si tratta di espressioni utilizzate a volte come sinonimiche a volte con accezioni diverse, la cui creazione e il cui uso sono stati accompagnati, almeno in Italia, da discussioni anche piuttosto accese sul miglior termine da utilizzare.

Credo non sia il caso qui di entrare nel dettaglio di un dibattito che ha, sicuramente, un valido fondamento ma che risulta penso secondario rispetto all'importanza di questa innovazione tecnologica in sé e soprattutto dei benefici che essa può portare al genere umano.

Per quanto mi riguarda userò – mi si perdoni la semplificazione - con valore generale il termine "telemedicina" e utilizzerò l'espressione "sanità elettronica" con riguardo a tutte quelle attività documentali, di carattere amministrativo, contabile, burocratico, prescrittivo, di conservazione e archivia-

[16] L'*health informatics* si concentra nell'applicazione dei sistemi informatici all'ambito sanitario. In questo settore, l'impiego dell'informatica può estendersi dal semplice utilizzo del computer come mezzo computazionale al processo di acquisizione, *storage*, *retrieval*, rappresentazione e manipolazione della conoscenza (*knowledge*). In altre parole, l'*health informatics* non si occupa solo di fornire le premesse tecnologiche a determinati servizi sanitari, ma si estende ai processi di *back office* e a quelli più generalmente amministrativi, si occupa di creare una rete di rapporti con gli altri enti sanitari e le farmacie, con le pubbliche amministrazioni e i soggetti sociali e può gestire la complessità dei flussi informativi (dai dati clinici fino a quelli economico-finanziari). Per ulteriori informazioni si veda V. L. Sauter al link http// www.umsl.edu/~sauter/health_informatics/what is.html.

zione, che non sono propriamente l'atto medico ma che l'atto medico accompagnano e che lo giustificano, supportano, memorizzano e contano sotto il profilo amministrativo.

E come sappiamo il nostro Sistema Sanitario Nazionale include moltissime applicazioni di questo tipo, che affiancano le attività più propriamente di cura, prevenzione e diagnosi. Tali applicazioni si stanno anch'esse informatizzando e telematizzando (si pensi al fascicolo sanitario elettronico, alla prescrizione elettronica, ai referti on line, all'invio telematico dei certificati medici).

L'importante è l'innovazione tecnologica in sé –dicevamo – al di là delle definizioni e soprattutto i benefici che essa può portare all'umanità. E la peculiare utilità dell'innovazione tecnologica telemedica è quella che essa ha "adottato" dalla telematica: il poter operare a distanza ma a prescindere dalla distanza stessa, e quindi il più tempestivamente possibile.

Nella telemedicina c'è sempre infatti un certa distanza spaziale (più o meno grande) tra il paziente e il medico – o altro operatore sanitario - ; tra il medico di medicina generale e lo specialista che egli intende consultare; tra gli specialisti "riuniti" a consulto; tra il tecnico che effettua la radiografia e chi la riceve a fini diagnostici (sia esso medico o paziente).

C'era grandissima distanza – in quella che viene descritta come la prima originaria applicazione - tra l'astronauta nello spazio e la stazione sulla Terra dove si trovava il sanitario che misurava i suoi parametri vitali e interveniva al bisogno, e c'è ancora enorme distanza spaziale tra il marinaio che si sente male in piena traversata e il medico sulla terra ferma che è incaricato di intervenire, e infine, nei casi più eclatanti e che hanno avuto maggior risonanza mediatica, tra il chirurgo che muovendo le mani dentro appositi guanti con sensori "dice" al robot cosa fare e il robot stesso che, a distanza anche di interi continenti, interpretando le indicazioni che gli giungono via rete, "opera" il paziente in una particolarissima sala operatoria telematica.

La distanza viene quindi annullata o accorciata dalla trasmissione telematica delle informazioni digitalizzate. Questa è la grande forza della telemedicina, che può consentirle interventi rapidi, spesso decisivi per la vita umana, in situazioni di emergenza o in condizioni in cui sarebbe impossibile un intervento medico di persona in tempo utile, ma che rende possibile anche, nelle situazioni

meno "estreme", risparmi di tempo, di energie umane e non, e pertanto in sintesi risparmi di spesa finora insperati.

La distanza – e il suo superamento – costituiscono dunque la forza delle applicazioni telemediche e, al tempo stesso, ne sono il limite.

Molti, giustamente, sottolineano come la cura e l'atto sanitario latamente intesi siano attività in cui un elemento determinante, per la stessa riuscita dell'intervento, sia il rapporto - anche fisico - che si instaura tra chi cura e chi viene curato, è l'interazione tra paziente e medico, anche nel suo lato visivo, corporeo, espressivo.

La necessità, che per forza di cose la tecnica ci impone, di una imprescindibile intermediazione del computer e della rete nelle applicazioni telemediche, non lo si può negare, rappresenta un limite cui non siamo abituati nella realtà non virtuale e rischia di introdurre un aspetto di spersonalizzazione in questa modalità di cura, di creare una sorta di schermo opaco in una relazione che il paziente avverte come strettissima: quella con il suo medico.

Il fatto è che come spesso succede le tecnologie non sono risposte assolute, sono occasioni che ci vengono proposte e che vanno utilizzate con criterio, misura, opportunità, ovviandone, per quanto possibile, i limiti e sfruttandone i punti di forza.

È sicuramente vero che una carezza consolatoria sincera da parte del nostro medico vale più di cento sue mail, ma una cosa non esclude l'altra e in molti altri casi tocca fare di necessità virtù.

Vi sono luoghi, situazioni, circostanze in cui il medico non ce la fa ad arrivare, o non ce la fa ad arrivare così frequentemente come ci occorrerebbe. In questi casi, avere la possibilità di mettersi in contatto con lui attraverso un monitor, sentire la sua voce, ascoltare i suoi consigli, mentre egli esamina il risultato delle misurazioni vitali che ci riguardano, diventa importante, anzi essenziale.

E questo vale non solo per il medico, ma anche per altri professionisti, per lo psicologo per esempio.

Lo psicologo che non ce la fa ad addentrarsi tutti i giorni nelle aspre terre di certe regioni italiane, può invece tutti i giorni mettersi in contatto con il suo assistito attraverso le rete e sentire come sta dalla sua viva voce, può parlargli quotidianamente e l'assistito sa che può contare su questo fatto (e così la sua

famiglia). Questo aiuta il paziente a sentirsi non abbandonato e aiuta la sua famiglia a sentirsi non sola nella sua condizione di disagio.

La possibilità tecnica di un contatto a grande distanza e in una molto più ampia fascia di ore e di giorni diviene così un elemento di vicinanza, di costante presenza, sia pure virtuale, di aiuto concreto.

La telemedicina è e rimane quindi prima di tutto e soprattutto un atto di cura e – sotto questo profilo - va sicuramente sposata la posizione di chi, in luogo di questo termine, preferisce usare l'espressione "medicina telematica", a sottolineare che, se è vero che le tecnologie sono un supporto fondamentale di questo tipo di erogazione sanitaria, essa rimane però fondamentalmente e principalmente un atto umano di un professionista, finalizzato alla cura di un altro essere umano.

Essa deve essere letta quindi non tanto come declinata dalle categorie logiche dell'informatica, dell'ingegneria, della telematica, ma da quelle della medicina, perché essa è fatta per l'uomo e per curare l'uomo.

6. La sua evoluzione

Con il trascorrere degli anni, l'ambito delle soluzioni applicative si è considerevolmente ampliato: l'erogazione a distanza di atti di cura, ma anche la comunicazione dei referti, la condivisione tra specialisti di informazioni cliniche per agevolare l'attività diagnostica, fino addirittura alla possibilità di realizzare a distanza un'operazione chirurgica, grazie alla telerobotica.

Della molteplicità dei possibili impieghi della telemedicina prese atto, *in primis*, l'Unione europea che nel 1990 stabilì che essa dovesse comprendere: "Il controllo, il monitoraggio e la gestione dei pazienti, nonché la loro educazione e quella del personale sanitario, attraverso l'uso di sistemi che consentano un tempestivo accesso alla consulenza di esperti e alle informazioni del paziente, indipendentemente da dove il primo o le seconde risiedano"[17].

La definizione UE di "telemedicina" mette dunque in evidenza come la sua finalità non sia solo quella di assicurare assistenza medica a pazienti distanti dai centri sanitari, agevolando la comunicazione paziente – medico - struttura sanitaria, ma anche quella di rendere adeguati ed aggiornati i servizi sanitari nazionali degli Stati membri, con particolare attenzione alla informazione e alla formazione del paziente e del personale sanitario e all'aggiornamento professionale di quest'ultimo.

L'anno successivo l'Organizzazione Mondiale della Sanità (WHO) definì la nuova scienza applicata in maniera più rigorosa come "l'erogazione di servizi di cura e assistenza, in situazioni in cui la distanza è un fattore critico, da parte di qualsiasi operatore sanitario attraverso l'impiego delle tecnologie informatiche e della comunicazione, per lo scambio di informazioni utili alla diagnosi, al trattamento e alla prevenzione di malattie e traumi, alla ricerca e per la formazione continua del personale sanitario, nell'interesse della salute dell'individuo e della comunità".

Progressivamente e sempre più fortemente, l'Unione europea venne a considerare l'evoluzione tecnologica - anche in senso telemedico - dei servizi socio-sanitari nazionali come un elemento strategico per il loro miglioramento e una delle soluzioni essenziali per far fronte all'aumento dei costi assistenziali e sanitari di una popolazione europea caratterizzata da un progressivo invecchia-

[17] Dal documento: *"Advanced Informatics in Medicine – AIM"* 1990.

mento e da cronicità delle patologie principali, in un quadro di crisi economica che si andava aggravando.

La stessa Unione, con l'*Action Plan e-Health* 2004, avvia una pianificazione condivisa fra gli Stati membri dei provvedimenti in materia telemedica da adottare entro il 2009[18].

Il piano si prefigge tre obiettivi cruciali: sviluppare strategie e metodologie comuni tra gli Stati membri, accelerare l'avvio della telemedicina attraverso azioni complessive, verificare i risultati delle esperienze attraverso la diffusione delle *best-practices* e la valutazione degli effetti quali-quantitativi dell'*e-Health*.

All'*Action Plan e-Health* 2004 hanno fatto seguito la Comunicazione della Commissione del 4 novembre 2008[19] e la Decisione della Commissione del 23 febbraio 2009, che adotta il Piano di lavoro per il 2009 per l'attuazione del secondo programma d'azione comunitaria in materia di salute (2008 - 2013) e che stabilisce i criteri di selezione e di attribuzione per l'erogazione dei contributi finanziari alle azioni di tale programma.

Nella Comunicazione del 2008, la Commissione europea prende atto che, nonostante il potenziale offerto dall'*e-Health*, i suoi innegabili vantaggi e la maturità tecnica delle sue applicazioni, il ricorso ai servizi telemedici è ancora limitato e il relativo mercato presenta tuttora un alto grado di frammentazione.

Il limite maggiore, secondo la Commissione, consiste nel fatto che la maggior parte delle iniziative in questo settore è rappresentata da progetti singoli e di piccola scala, che stentano ad integrarsi nel sistema di assistenza sanitaria.

Con il documento in esame, la Commissione si prefigge di supportare gli Stati membri nella difficile opera di procedere all'integrazione dell'*e-Health* con i sistemi nazionali di assistenza sanitaria. Per dirlo con le sue stesse parole: si propone di "fornire elementi atti a creare fiducia e di favorire l'accettazione" dei servizi di telemedicina presso i singoli Stati membri.

[18] Comunicazione della Commissione europea *"e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area 2004"*, 30 maggio 2004.

[19] "Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato europeo, al Comitato economico e al Comitato delle Regioni sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società" COM (2008) 689.

Accanto a questo primario obiettivo, e con funzione strumentale rispetto ad esso, la Commissione europea, consapevole che "soltanto pochi Stati membri hanno assetti normativi chiari su cui si fonda l'esercizio della telemedicina", ritiene indispensabile contribuire ad "apportare chiarezza del diritto". Ed un primo baluardo giuridico che dovrà essere riconosciuto dagli Stati è quello di adeguate garanzie a "tutela dei dati personali, nonché le più elevate norme di sicurezza per i pazienti".

Un altro punto importante, e che non va trascurato, a giudizio della Commissione è quello secondo cui "la prestazione transfrontaliera dei servizi di telemedicina – frequente in questo tipo di tecnologia – richiede anch'essa chiarezza giuridica", specie per quanto riguarda la tutela dei dati personali.

Il terzo *step* consisterà nel risolvere i problemi tecnici secondo parametri necessariamente interoperabili e agevolare lo sviluppo del mercato di queste soluzioni tecnologiche.

Per quanto concerne la decisione della Commissione del 23 febbraio 2009, il Piano di lavoro al paragrafo 3.2.2.2, rubricato "Migliorare la sicurezza dei pazienti mediante un'assistenza sanitaria sicura e di alta qualità", prevede l'attuazione dell'azione prevista dalla Comunicazione 689 del 2008 or ora citata al fine di "aumentare la fiducia nella telemedicina e l'accettazione delle stessa, tenendo conto anche degli aspetti etici e di quelli connessi alla sfera privata".

Considerato che per "rafforzare la consapevolezza, la fiducia e l'accettazione da parte delle autorità sanitarie, dei professionisti e dei pazienti", risulta indispensabile fornire prove scientifiche dell'efficacia della telemedicina anche sotto il profilo del risparmio di spesa, la Commissione ritiene indispensabile avviare una sperimentazione ad ampio raggio.

D'altro canto, il governo europeo riconosce che le imprese del settore – spesso piccole e medie – non sono in grado di fornire la capacità finanziaria necessaria per effettuare sperimentazioni su larga scala. Al fine, quindi, di valutare l'efficienza della telemedicina, anche sotto il profilo dei costi, si procederà ad una valutazione fondata sul lavoro di esperti, su studi effettuati per conto della Commissione, su progetti pilota su larga scala e su sperimentazioni pertinenti.

Ecco che, a questo scopo, la Commissione prevede e regolamenta "un deciso intervento del settore pubblico" per supportare finanziariamente le imprese europee che si dedicano alla telemedicina.

Sotto il profilo della certezza del diritto, la Commissione si prefigge di pubblicare, in collaborazione con gli Stati membri, un'analisi del quadro giuridico comunitario applicabile ai servizi di telemedicina.

La stessa Commissione conclude la Comunicazione affermando: "È tempo che la telemedicina migliori la vita dei pazienti ed offra nuovi strumenti ai professionisti della sanità: la telemedicina può essere d'aiuto ad affrontare le sfide principali per i sistemi sanitari e può offrire opportunità considerevoli all'industria europea".

L'Unione europea riconosce, tuttavia, la necessità della collaborazione degli Stati membri laddove afferma: "La telemedicina realizzerà il suo pieno potenziale unicamente se gli Stati membri si impegneranno attivamente ad integrarla nei loro sistemi sanitari". Gli Stati membri vengono quindi da adesso in poi coinvolti in prima persona.

CAPITOLO SECONDO
IL TRATTAMENTO DEL DATO SANITARIO

1. Il trattamento del dato

Il trattamento dei dati è oggi disciplinato, quale regola fondamentale, dal Codice della privacy (d.lgs. 196/2003). Il Codice regolamenta il trattamento dei dati *personali*.

Per dato personale si deve intendere il dato costituito da un contenuto informativo riferito ad una determinata persona fisica, identificata o identificabile.

In particolare, ai sensi dell'art. 4 "Per *dato personale* si intende qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"[20].

Sono pertanto sicuramente esclusi dall'ambito applicativo del Codice della privacy tutti quei casi in cui si abbia a che fare con una quantità (anche molto grande) di dati che però, per quanto possano essere vari, complessi e anche estremamente interessanti, non fanno riferimento ad una persona fisica, ma

[20] Articolo 4 comma 1 lettera b. Il presente articolo é stato recentemente così modificato dal cosiddetto "Decreto Monti", decreto legge 6 dicembre 2011 n. 201, convertito con legge n. 214 del 22 dicembre 2011, pubblicato in G.U. del 6 dicembre 2011, in vigore dallo stesso giorno. La precedente versione del citato articolo prevedeva: "Per dato personale si intende qualunque informazione relativa a persona fisica, *persona giuridica, ente od associazione,* identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Il Decreto Monti ha quindi introdotto una importante modifica: devono essere considerati dati personali solo i dati delle persone fisiche, non quelli delle persone giuridiche, degli enti e delle associazioni. Lo scopo della riforma è quello di introdurre semplificazioni, soprattutto nei rapporti tra le imprese: tutta una serie di adempimenti che erano estesi precedentemente anche alle persone giuridiche e agli enti, primo fra tutti l'informativa e la raccolta del consenso, vanno ora effettuati solo a tutela delle persone fisiche. Per quanto sia comprensibile l'obiettivo perseguito mi trovo a non concordare pienamente con la tecnica legislativa utilizzata: per introdurre semplificazioni burocratiche non è sempre opportuno arrivare a negare l'esistenza di una categoria giuridica: in questo caso quella di ente/soggetto interessato che ha dati suoi propri che anch'essi, almeno tanto quelli delle persone fisiche, devono essere fatti oggetto di tutela. Va tuttavia segnalato, in positivo, che con questa modifica della norma ci allineiamo alla condizione di molti Stati membri dell'Unione, per la cui normativa privacy l'interessato è solo una persona fisica.

sono anonimi, si riferiscono a soggetti indeterminati, a categorie o gruppi di persone.

In questo caso non dobbiamo preoccuparci: il Codice della privacy non va applicato. Si suole dire pertanto che le norme sulla privacy si applicano ai dati personali, ma non ai dati anonimi o aggregati.

Cosa si deve intendere per trattamento del dato? Il trattamento, ai sensi del Codice della privacy, nonché, prima di lui, della normativa europea che lo ispira, è un concetto molto ampio e omnicomprensivo.

Per trattamento, infatti, si deve intendere, ai sensi dell'art. 4 comma 1 lettera a "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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 di dati, anche se non registrati in una banca di dati".

Si tratta, come si può ben vedere, di una definizione che include tutti i possibili destini e tutte le possibili "fasi di elaborazione" di un'informazione. E questo per offrire la maggior possibile tutela a colui cui il dato si riferisce.

Data l'ampiezza della definizione, non è possibile distrarsi: in quasi tutti i casi in cui usiamo un dato personale, possiamo essere certi che tale "uso" costituisca un trattamento e che pertanto sia necessario osservare le norme del Codice privacy.

Sicuramente un modo prevalente di "usare" un dato personale è quello scritto, che comporta la sua annotazione in documenti e pertanto tutta una serie di trattamenti documentali dei dati, con conseguenti problemi di archiviazione e conservazione di tali documenti.

Così come, sicuramente, molti di tali documenti sono oggi documenti informatici, per cui ci troviamo a dover trattare dati personali espressi in formato digitale e a dover applicare non solo le norme del Codice della privacy ma anche le altre del nostro ordinamento che riguardano il documento digitale, la sua firma, la sua trasmissione, la sua archiviazione e la sua conservazione[21].

[21] Per un approfondimento si rimanda a C. Rabbito, Sanità elettronica e diritto: problemi e prospettive, SEU – Società Editrice Universo, Roma, 2010.

Ma non dobbiamo pensare che il trattamento di un dato personale sia da ridurre semplicisticamente al documento scritto, sia esso cartaceo o informatico.

Il trattamento del dato è infatti "qualunque operazione" riguardi il dato, anche se si tratta di una operazione non scritta. Anche, per esempio, se il trattamento è orale o visivo è comunque un trattamento ai sensi del Codice della privacy. Pensiamo ad una telefonata, ad una comunicazione audiovisiva via internet, ad un discorso convegnistico, alla stessa – per estremizzare - semplice annotazione di un dato in un foglietto attaccato al nostro monitor in ufficio.

Quindi attenzione: se trattiamo dati che non sono necessariamente scritti in un foglio o in un file questo non significa che siamo salvi dall'osservanza delle norme privacy.

In particolare, ai sensi dell'art. 2 "Il trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

2. I "protagonisti" della privacy

Il protagonista assoluto della normativa privacy è indubbiamente l'*interessato*. L'interessato è la persona fisica cui si riferiscono i dati personali[22].

L'interessato non è solo il soggetto cui i dati si riferiscono, ma anche il soggetto che principalmente ha voce in capitolo circa il loro uso e il loro destino e che è fatto oggetto di massima tutela con riguardo al trattamento dei suoi dati.

Egli è il soggetto che, ricevuta la debita informativa, deve esprimere il proprio consenso affinché quei dati possano essere trattati.

Un altro soggetto di grande importanza in ambito privacy è il *titolare*.

Per titolare si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare (il cosiddetto *contitolare*), le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

[22] Per un approfondimento sulla natura dell'interessato si legga la nota precedente.

La lettura di tale definizione fa comprendere come in moltissimi ambiti, quali per esempio quello della Pubblica Amministrazione, della Sanità e nel mondo imprenditoriale, il titolare, per quanto legalmente rappresentato da una persona fisica (direttore, dirigente di area, amministratore delegato, presidente etc…) è di fatto un ente, una persona giuridica.

In molti casi non bisogna cercare, quindi, nell'informativa, alla indicazione "titolare" un nome e un cognome, ma l'indicazione della persona giuridica, del'ente, dell'associazione, la ditta dell'impresa che trattano i dati, cui seguiranno, per maggiore tutela dell'interessato, il nome e il cognome del loro legale rappresentante.

Altro personaggio di notevole rilievo nello scenario in cui ci stiamo muovendo è il *responsabile*.

È *responsabile* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Il responsabile, nel trattamento dei dati, deve quindi attenersi alle istruzioni che gli impartisce il titolare dei dati, in quanto soggetto cui competono le decisioni circa tale trattamento e la relativa responsabilità giuridica.

Al fine di vincolare il responsabile alle sue indicazioni, è opportuno che il titolare predisponga un atto scritto di nomina, in cui il titolare, nel corpo dell'atto o nell'allegato, indicherà i requisiti fondamentali di tale trattamento, cui il responsabile si dovrà attenere[23].

Possono esservi anche dei responsabili dei dati che sono nominati dal titolare al di fuori della sua struttura: in questo caso si parla di "responsabili esterni", la cui nomina avviene con modalità analoghe a quelle dei responsabili interni[24].

Sono responsabili esterni, per esempio, i soggetti cui il titolare o il responsabile interno (per indicazione del titolare) affidano alcune mansioni specifiche e determinate, con carattere altamente tecnico. Si pensi per esempio all'attività di conservazione e archiviazione dei documenti digitali, all'attività di manutenzione e aggiornamento del sistema informatico, al provider che consente al titolare l'accesso alla rete Internet.

[23] Un esempio di nomina del responsabile si può trovare nell'appendice, allegato n. 1.

[24] Un esempio di nomina di responsabile esterno si trova nell'appendice all'allegato n. 2.

Si tratta spesso di attività di carattere tecnico informatico che vengono affidate dal titolare- impresa o dal titolare-pubblica amministrazione all'esterno, o – come si suole dire – in *outsourcing*.

Ma non vengono delegate a responsabili esterni solo operazioni connesse all'informatica e alla telematica. È responsabile esterno dei nostri dati il nostro commercialista, per esempio, o la società di revisione contabile di un'azienda.

Tornando ai personaggi fondamentali della privacy, vi sono poi coloro che, legati al titolare da un rapporto di lavoro – latamente inteso e variamente configurabile – prestano la loro opera a suo favore e materialmente e concretamente mettono mano ai dati nell'ambito della loro mansione.

Si tratta dei cosiddetti "incaricati del trattamento", che sono così definiti dall'art. 30 del Codice della privacy: «Art. 30 (Incaricati del trattamento): 1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. 2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima».

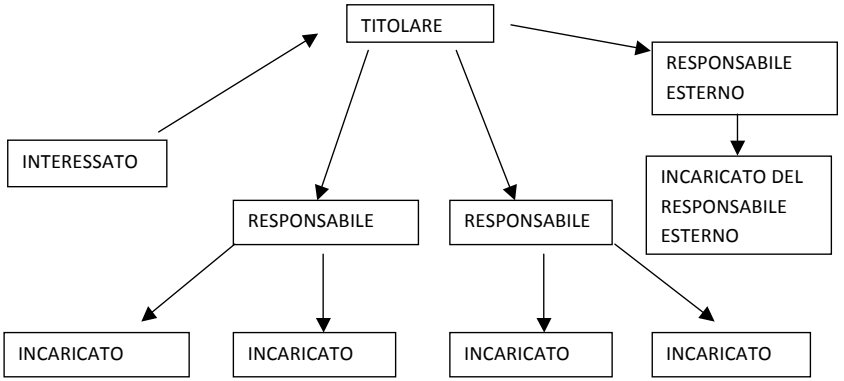
Gli incaricati sono dunque sempre persone fisiche: si tratta delle persone che sono autorizzate dal titolare o dal responsabile a compiere le operazioni di trattamento dei dati.

Tale autorizzazione deve necessariamente avvenire per iscritto e può assumere la forma della lettera d'incarico[25] o di lettera di riservatezza[26].

Si utilizza in particolare la lettera di riservatezza nel caso in cui l'incaricato operi sui dati in via temporanea o per un periodo di tempo limitato: si pensi per esempio ai casi di uno stagista – che rimane per il solo periodo dello stage -, ad un ricercatore, che ha necessità di consultare i dati solo ai fini della ricerca che sta conducendo, a chi è vincolato da un contratto di prestazione occasionale e non da un rapporto di lavoro subordinato a tempo indeterminato, o ad uno studioso venuto in visita.

[25] Un esempio di lettera d'incarico è contenuto nell'allegato 3.

[26] Un esempio di lettera di riservatezza è contenuto nell'allegato 4.



3. L'informativa e il consenso

Il nostro Codice della privacy prevede, quale principio generale e salvo specifiche, regolamentate eccezioni, che il trattamento del dato personale possa avvenire solo previo consenso dell'interessato.

Tale consenso deve essere necessariamente informato, ovvero l'interessato, per poter esprimere un valido consenso, deve essere stato reso consapevole del tipo e delle caratteristiche del trattamento, nonché dei diritti che egli può esercitare circa tale trattamento.

Si tratta di un principio affermato già nella direttiva europea di cui il nostro Codice rappresenta il recepimento. Si legga infatti l'art. 2 par. 1 lett. h della dir. n. 95/46/CE: il consenso è "qualsiasi manifestazione di volontà libera, specifica e *informata* con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento".

Ai sensi dell'art. 7 della stessa direttiva gli Stati membri devono regolamentare la materia in modo che *in primis* il trattamento di dati personali possa essere effettuato soltanto quando "la persona interessata ha manifestato il proprio consenso in maniera inequivocabile".

Vi sono poi casi, specificamente regolamentati, in cui il legislatore consente il trattamento del dato a prescindere da un esplicito consenso dell'interessato: quando il trattamento:

b) è necessario all'esecuzione del contratto concluso con la persona interessata,
c) è necessario per adempiere un obbligo legale,

d) *è necessario per la salvaguardia dell'interesse vitale della persona interessata*,
e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri,
f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

L'elaborazione e messa a disposizione dell'interessato di una informativa adeguata e per quanto possibile completa è un adempimento fondamentale in vista del trattamento.

Ai sensi del nostro Codice[27] l'informativa deve contenere:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti dell'interessato ex articolo 7[28];
f) gli estremi identificativi del titolare e del responsabile.

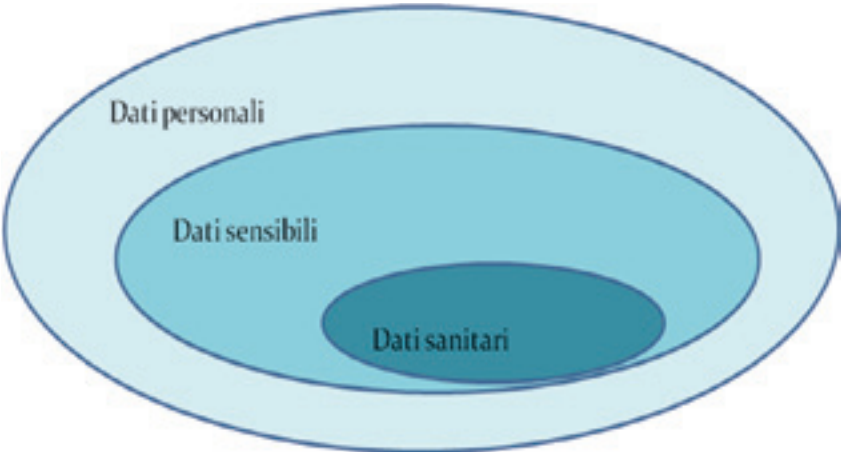
[27] Articolo 13.

[28] Art. 7. Diritto di accesso ai dati personali ed altri diritti 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. 2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. 3. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. 4. L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

4. Il dato sanitario

Nell'ambito dei dati personali esiste una particolare categoria di cosiddetti "dati sensibili".

Il nostro Codice definisce "dati sensibili" i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché *i dati personali idonei a rivelare lo stato di salute e la vita sessuale*.



Il Codice fa oggetto di particolare tutela i dati sensibili, proprio in considerazione della loro natura.

Nell'ambito di questa speciale categoria di dati, come si desume dalla lettera della norma, il legislatore include anche *i dati personali idonei a rivelare lo stato di salute*, cioè i dati personali a contenuto sanitario.

A tali dati vanno applicate le norme di particolare tutela previste per i dati sensibili, salvo che essi non siano trattati *al fine della tutela della salute dell'interessato, di terzi soggetti o della collettività* e il loro trattamento sia *effettuato da specifici titolari qualificati, i quali istituzionalmente svolgono funzioni di tutela della salute, ossia gli esercenti delle professioni sanitarie e degli organismi sanitari pubblici.*

In tale caso non siamo più in presenza della categoria giuridica di dato sensibile, ma di una categoria caratterizzata da ancora maggiore specialità: si tratta dei *dati sanitari*.

Pertanto, sono dati sanitari i dati sensibili che recano informazioni circa lo stato di salute dell'interessato e che vengono trattati per la tutela della salute dell'interessato stesso, dei terzi o della collettività da organismi sanitari o da esercenti le professioni sanitarie.

Qualora tutte queste condizioni siano verificate, e cioè si sia in presenza di dati sanitari, le norme che devono essere applicate non sono quelle "genericamente" relative ai dati sensibili, ma quelle specificamente riferite ai dati sanitari contenute nel Titolo V della Parte Seconda, artt. 75 e seguenti del Codice.

Secondo la dottrina non sono dati sanitari solo quelli che si riferiscono ad un determinato stato patologico dell'individuo, ma più genericamente quelli che riguardano "lo stato di salute" dell'interessato.

Si può ritenere, quindi, che essi comprendano tutte le informazioni relative allo stato fisico, psichico e relazionale dell'individuo.

La salute alla quale si devono riferire i dati per essere qualificati come "sanitari" è infatti uno *status* globale dell'individuo, che si estende all'elemento psicologico, fisico e relazionale[29].

Circa i soggetti che sono chiamati a trattare tali dati a fini di salute, si ritiene che debbano qualificarsi come "esercenti professioni sanitarie" coloro che svolgono la loro attività a stretto contatto con il paziente e che la esercitano sulla base di un titolo, in qualsiasi forma rilasciato dalla pubblica autorità a fini abilitativi, quali: medici chirurgi, odontoiatri, farmacisti, ostetrici, assistenti sanitari, infermieri professionali, vigilatori d'infanzia, terapisti della rianimazione, tecnici sanitari di radiologia medica, tecnici di immunologia e trasfusione, tecnici di igiene ambientale, igienisti dentali, podologi, audiometristi, massofisioterapisti, tecnici della riabilitazione funzionale, tecnici di laboratorio, dietisti.

[29] Si leggano in proposito J. Monducci, G. Sartor, Codice in materia di dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003, n.196, Cedam, 2004 e J. Monducci, Diritti della persona e trattamento dei dati particolari, Giuffré, 2003.

Per quanto concerne gli "organismi sanitari pubblici" deve ritenersi che rientrino in tale definizione le strutture sanitarie individuate dalla legge 23 dicembre 1978 n. 833 e successive modifiche.

Si tratta di: Aziende Sanitarie Locali, Aziende ospedaliere, istituti di ricerca e cura a carattere scientifico, farmacie pubbliche, ambulatori destinati a fornire prestazioni sanitarie mediche e chirurgiche, enti di ricerca e sperimentazione, residenze sanitarie e assistenziali.

Nel caso di trattamento dei dati da parte di esercenti le professioni sanitarie che operano in virtù di un rapporto contrattuale con la struttura sanitaria tale trattamento va ricondotto a quello degli organismi sanitari di riferimento: il professionista che opera all'interno della struttura non agisce quale titolare del trattamento, poiché titolare è l'organismo sanitario, bensì in qualità di incaricato o di responsabile e come tale deve essere specificamente individuato e nominato.

D'altro canto, se il trattamento di dati a contenuto sanitario non è effettuato come richiesto dal legislatore a fini di tutela della salute, ma con altri scopi, per esempio a fini di ricerca scientifica, a fini amministrativi, contabili, di controllo di gestione, di erogazione di prestazioni non deve applicarsi la disciplina relativa ai dati sanitari, bensì quella che si occupa dei dati sensibili di cui agli artt. 20 e 26 del Codice privacy.

Si potrebbe dire, per semplificare, che se un dato a contenuto sanitario non è trattato da organismi sanitari o esercenti professioni sanitarie e non è trattato a fini di tutela della salute, esso "passa di categoria" e viene fatto rientrare nuovamente nel più vasto insieme dei dati sensibili.

5. Quando e come il dato sanitario può essere trattato

In considerazione della estrema delicatezza del dato sanitario, la regolamentazione del suo trattamento, in ambito internazionale e poi a livello comunitario, è stata conformata al principio del *generale divieto* del trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale - specie con riguardo al loro trattamento con mezzi informatici e telematici - a meno che il diritto interno non predisponesse idonee misure di garanzia.

In particolare, la Convenzione del Consiglio d'Europa n. 108 del 1981[30] ha previsto che tali dati *non possano essere elaborati automaticamente* "a meno che il diritto interno non preveda garanzie appropriate".

La direttiva 95/46/CE[31], che introduce nella Comunità Europea, come abbiamo visto, la prima regolamentazione della privacy, si conforma a quanto stabilito dal Consiglio d'Europa, ma prevede una specifica eccezione al divieto di trattamento nel caso in cui questo sia effettuato da personale medico assoggettato per legge all'obbligo del segreto professionale e tale trattamento sia necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri cura.

Già nella legge italiana di recepimento della direttiva, la 675 del 1996, il nostro legislatore adegua la disciplina dei dati sanitari a quanto indicato dal legislatore europeo, allo scopo di bilanciare la necessità di tutelare la vita e l'incolumità personale con il diritto alla riservatezza.

L'attuale Codice, all'art. 76 primo comma, prevede che gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possano trattare i dati idonei a rivelare lo stato di salute:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati ed operazioni indispensabili per perseguire una *finalità di tutela della salute o di incolumità fisica dell'interessato*;
b) anche senza il consenso dell'interessato, ma rispettando la previa autorizzazione del Garante, se il trattamento è svolto per *finalità di tutela della salute o dell'incolumità di un terzo o della collettività*.

Per verificare la necessità di applicazione dell'articolo sopra riportato, è molto importante tenere conto della finalità per cui si intendono trattare i dati e del tipo di dati da trattare:

- nel caso in cui il trattamento sia finalizzato alla tutela della salute e dell'incolumità dell'interessato, di un terzo o della collettività si dovrà applicare l'art. 76; nel caso in cui in relazione agli stessi dati le finali-

[30] Convenzione di Strasburgo n. 108/1981, ratificata nel nostro paese con la legge 21 febbraio 1989, n. 98, art. 6.

[31] Articolo 8 comma 3 della Direttiva 95/46/CE.

tà del trattamento siano diverse (amministrative, gestionali, etc…), si rientrerà nell'ambito dell'art. 20, applicabile in presenza delle rilevanti finalità di interesse pubblico indicate dall'art. 85;

- qualora l'organismo sanitario debba procedere al trattamento di dati sensibili diversi dai dati sanitari, è tenuto al rispetto delle condizioni di cui all'art. 20 del Codice.

Il dato sanitario del paziente non può quindi essere trattato senza il suo consenso, ma a tutela della salute e dell'incolumità altrui (di un'altra persona o dell'intera collettività) l'art. 76 comma 1 lett. b, permette il trattamento senza il consenso dell'interessato, qualora vi sia l'autorizzazione del Garante, fermi restando i limiti della finalità allo scopo e della indispensabilità, nonché il divieto di diffusione dei dati sanitari.

Per il rilascio dell'autorizzazione si richiede ex art. 76 che il Garante acquisisca il parere del Consiglio Superiore di Sanità. Tale parere non è tuttavia vincolante e può essere omesso nei casi di particolare urgenza.

Il Garante rilascia periodicamente un'autorizzazione generale attinente ai dati relativi allo stato di salute e alla vita sessuale. Tale autorizzazione generale consente il trattamento dei dati sanitari per finalità di tutela della salute di un terzo o della collettività nel caso in cui l'interessato non abbia prestato il consenso o non possa prestarlo per irreperibilità.

Il consenso al trattamento del dato sanitario potrà essere raccolto solo previo rilascio di un'adeguata informativa[32].

L'informativa dovrà essere resa *in forma chiara*, evidenziando gli elementi di cui all'art. 13. Essa dovrà essere resa preferibilmente per iscritto, anche con carte tascabili con eventuali pieghevoli.

L'informativa dovrà contenere l'analitica indicazione dei trattamenti effettuabili per scopi scientifici, ovvero mediante l'uso delle moderne tecnologie, ivi comprese telemedicina e teleassistenza, nonché per fornire beni o servizi mediante rete telematica, al fine di notiziare l'interessato dei trattamenti che più di altri presentano rischi per i diritti e le libertà fondamentali[33].

[32] Esempi di modelli di rilascio dell'informativa e di raccolta del consenso al trattamento del dato sanitario sono reperibili negli allegati 5, 6 e 7.

[33] Si vedano gli articoli 78 e 79 del Codice. Le precauzioni relative alla telemedicina e alla teleassistenza

6. Il consenso dell'incapace e l'emergenza sanitaria

Il nuovo Codice privacy consente, sia pure in circostanze particolarissime, che il consenso al trattamento del dato sanitario venga prestato non direttamente dal paziente ma da soggetti terzi.

Se, in particolare, il trattamento sia necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato e questi non possa prestare il proprio consenso per *impossibilità fisica*, *incapacità d'agire* o *incapacità di intendere e di volere*, il consenso può essere manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, dal convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato[34] (art. 24 comma 1 lett. e).

Nel caso in cui, poi, il paziente si trovi in stato di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, e *non sia stato possibile acquisire il consenso da chi esercita legalmente la potestà*, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato, *si potranno posticipare informativa e consenso*.

Tuttavia non appena ve ne sia la possibilità l'informativa dovrà essere data e il consenso dovrà essere raccolto presso il paziente o presso chi può darlo per lui.

L'art. 82 del Codice prevede infatti la possibilità per i titolari qualificati di *procedere al trattamento senza il consenso dell'interessato o di terzi abilitati*, salvo poi l'obbligo di procurarselo una volta cessate le ragioni di urgenza[35].

Tale norma, applicabile sia agli esercenti le professioni sanitarie e agli organismi sanitari pubblici, sia agli organismi sanitari privati e ai servizi o strutture di organismi pubblici diversi dagli organismi sanitari operanti in ambito sanitario o della sicurezza del lavoro, è stata introdotta in ragione del fatto che in ambito sanitario ci si trova spesso nella necessità di dover trattare dati sanitari senza

sono previste dal legislatore con riferimento ai soli casi di utilizzo delle modalità semplificate di rilascio dell'informativa e di raccolta del consenso – per le modalità semplificate si legga il seguito della trattazione – ma ritengo che, in presenza di un sempre più massiccio impiego dell'informatica e della telematica nella Sanità, sia opportuno provvedere sempre ad avvertire il paziente.

[34] Art. 24 comma 1 lett. e

[35] Per un approfondimento si rimanda a pag. 85 e seguenti.

che materialmente o giuridicamente sia possibile acquisire il consenso dell'interessato.

Ai sensi dell'art. 82 l'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di *emergenza sanitaria o di igiene pubblica* per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31 marzo 1998, n. 112.

Inoltre, l'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di *rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato*.

Infine il legislatore consente che l'informativa e il consenso siano presentati e raccolti successivamente alla prestazione nel caso di *prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso*, in termini di tempestività o efficacia.

Come precedentemente accennato, laddove invece l'organismo sanitario debba procedere al trattamento di dati sensibili diversi dai dati sanitari[36], è tenuto al rispetto delle condizioni di cui all'art. 20 del Codice: il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nei casi in cui la disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili trattati e le operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici dai soggetti che effettuano il trattamento in relazione alle specifiche finalità perseguite nei singoli casi, con atto di natura regolamentare.

Tuttavia, se il trattamento non è previsto espressamente da una disposizione di legge, i soggetti pubblici possono richiedere al Garante l'individuazione delle

[36] Si ricordi che sono dati sensibili anche tutti i dati a contenuto sanitario non finalizzati alla tutela della salute dell'interessato, di un terzo o della collettività, ma esemplificativamente impiegati nell'ambito della funzione amministrativa, di gestione del personale, in ambito finanziario, contabile, di controllo di gestione e di previsione di bilancio.

attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili (art. 20 comma 3).

7. Le modalità semplificate di rilascio dell'informativa e di raccolta del consenso

Come si è potuto evincere da quanto detto finora, la modulistica che deve essere predisposta e fatta firmare da parte degli organismi sanitari e dagli esercenti le professioni sanitarie al fine di poter trattare i dati sanitari dei loro pazienti è piuttosto articolata e richiede un discreto impegno di tempo e di energie.

Il legislatore se ne è mostrato consapevole prevedendo, per gli organismi sanitari e per gli esercenti professioni sanitarie, modalità semplificate di rilascio dell'informativa e di raccolta del consenso.

Ai sensi dell'art. 77, di tali modalità semplificate possono avvalersi tanto gli organismi sanitari pubblici, quanto gli organismi privati, sia gli esercenti le professioni sanitarie, che altri soggetti pubblici che operano in ambito sanitario, della prevenzione e della sicurezza del lavoro.

Il riferimento "agli altri organismi privati" deve intendersi naturalmente rivolto "agli organismi privati sanitari": le agevolazioni previste dal Codice sono, infatti, da intendersi applicabili anche ai soggetti privati non operanti in regime di accreditamento o convenzione con il Servizio Sanitario Nazionale.

L'art. 78 del Codice disciplina le modalità semplificate di cui possono avvalersi il medico di medicina generale e il pediatra di libera scelta per rendere l'informativa.

Innanzitutto, il medico di base e il pediatra possono fornire un'unica informativa in relazione a più trattamenti, cioè a tutti i trattamenti, finalizzati alla prevenzione, alla diagnosi, alla cura, alla riabilitazione, svolti dallo stesso titolare o da terzi da lui incaricati, ma pur sempre nell'interesse del paziente.

L'art. 78 comma 4 consente che l'informativa esplichi i suoi effetti anche in relazione a trattamenti di dati correlati a quelli del titolare e effettuati da professionisti terzi, in quanto sostituti del titolare stesso o che svolgono l'attività

professionale in forma associata, che forniscono una prestazione richiesta dal titolare (per esempio un medico specialista) o i farmaci da lui prescritti.

La norma prescrive infatti che l'informativa del medico di medicina generale o del pediatra possa riferirsi:

a) al complessivo trattamento di dati personali necessario per l'attività di prevenzione, diagnosi, cura e riabilitazione svolte dal medico o dal pediatra,
b) al trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da un altro soggetto che:
   - sostituisce temporaneamente il medico o il pediatra,
   - fornisce una prestazione specialistica su richiesta del medico o del pediatra,
   - tratta i dati nell'ambito di un'attività professionale prestata in forma associata,
   - fornisce i farmaci prescritti.

Dal punto di vista contenutistico non paiono essere state introdotte particolari semplificazioni.

Tuttavia, nell'ottica di un sempre maggiore e più invasivo impiego delle tecnologie informatiche e telematiche, è previsto che, oltre agli elementi richiesti dall'art. 13, l'informativa dovrà contenere *l'analitica indicazione dei trattamenti effettuabili per scopi scientifici, ovvero mediante l'uso delle moderne tecnologie*, ivi comprese *telemedicina e teleassistenza*, nonché il fatto che potrà fornire beni o servizi mediante rete telematica[37].

Quanto sopra è stato previsto a tutela del paziente, al fine di rendergli nota la possibilità di un aumento dei rischi per la sua privacy, a seguito dell'applicazione delle nuove tecnologie al trattamento dei suoi dati sanitari (oltre naturalmente ad un indubbio incremento dei possibili vantaggi).

Le modalità semplificate per l'informativa riguardano anche, come accennato, gli organismi sanitari pubblici e privati e i servizi e i settori di soggetti pubblici che operano in ambito sanitario o della prevenzione e sicurezza del lavoro (art. 80 comma 1).

[37] Si veda in proposito la nota n. 33.

In tal caso, l'informativa potrà riferirsi ad una pluralità di prestazioni erogate anche da distinti reparti o unità dello stesso organismo, ovvero di più strutture ospedaliere o territoriali specificamente indicate; inoltre potrà avere ad oggetto una pluralità di trattamenti a favore dello stesso paziente, effettuati addirittura in tempi diversi.

La lettera della norma prevede infatti che, per quanto concerne l'informativa resa da organismi sanitari essa può essere resa in forma unica per:

a) una pluralità di trattamenti effettuati anche il luoghi territorialmente differenti oltre che in settori, reparti ed altre articolazioni operative di una stessa struttura sanitaria, ma queste andranno specificamente indicate nell'informativa;
b) avere ad oggetto una pluralità di trattamenti effettuati anche a fini amministrativi e addirittura in tempi diversi.

Oltre ad una semplificazione in relazione ad una molteplicità di soggetti che possono fornire la stessa informativa o ad una informativa che comprenda più trattamenti diversificati o che si susseguono nel tempo, sono state previste e regolamentate anche modalità semplificate di raccolta del consenso.

L'art. 81 dispone, infatti, che il consenso può:

a) essere manifestato in un'unica dichiarazione per tutti i trattamenti che saranno necessari e che può anche essere reso oralmente (purché venga annotato per iscritto dal sanitario), con deroga espressa alla regola generale che, per i dati sensibili, richiede la forma scritta per la stessa validità giuridica della raccolta.
b) avere ad oggetto una pluralità di trattamenti effettuati anche a fini amministrativi e addirittura in tempi diversi.

A questi fini, l'informativa e il consenso dovranno essere annotati dall'organismo o dalle strutture con modalità omogenee e coordinate e tali da permetterne la verifica da parte degli altri reparti o unità che trattano i dati dell'interessato anche in tempi diversi.

8. Le misure comportamentali a tutela della privacy del paziente

Il Codice della privacy, con riguardo al trattamento dei dati sanitari, introduce particolari indicazioni e comportamenti precauzionali a tutela della

privacy e della dignità del paziente che è sicuramente opportuno menzionare in questa sede.

Più specificamente, l'art. 83 del Codice sollecita i titolari di trattamenti in ambito sanitario ad adottare, nell'organizzazione delle prestazioni e dei servizi, misure di sicurezza idonee, finalizzate anche al rispetto del segreto professionale.

Sono qualificate come tali "le soluzioni finalizzate alla *massima tutela della dignità dell'interessato*, soprattutto in quelle particolari situazioni in cui il suo contatto con la struttura sanitaria avviene in concomitanza con una moltitudine di altri soggetti, i quali sia pure accidentalmente, potrebbero venire a conoscenza delle informazioni sanitarie che lo riguardano".

Si richiede pertanto l'adozione di soluzioni volte ad impedire, in occasione dei colloqui con l'operatore sanitario, l'*indebita conoscenza da parte di terzi dei dati personali del paziente* e l'impiego di prassi che, in occasione di prestazioni sanitarie o di adempimenti amministrativi, consentano il *mantenimento delle cosiddette "distanze di cortesia"* e di soluzioni che prescindano dall'individuazione nominativa degli interessati.

Per esempio ci si deve preoccupare che le visite mediche e la raccolta dei dati anamnestici dei pazienti non avvengano in situazioni di promiscuità con altri pazienti.

Inoltre, ai sensi dell'art. 84, le notizie relative al suo stato di salute possono essere comunicate al paziente non da chiunque o da un qualunque membro del personale della struttura sanitaria, ma esclusivamente da personale competente: i dati sanitari possono essere resi noti all'interessato, cioè, solo per il tramite di un medico designato dall'interessato o dal titolare del trattamento (es. la struttura ospedaliera).

Il secondo comma dello stesso articolo, tuttavia, consente al titolare o al responsabile del trattamento di autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici (es. l'assistente sanitario, l'ostetrica, l'infermiere professionale), purché gli stessi nell'esercizio dei propri compiti intrattengano rapporti diretti con i pazienti e siano stati nominati incaricati del trattamento con appropriate modalità e cautele, rapportate al contesto nel quale è effettuato il trattamento di dati.

Viene fatta però un'eccezione alla regola generale per cui i dati sanitari che riguardano il suo stato di salute possono essere comunicati *solo* all'assistito - diretto interessato: è previsto infatti che notizie sullo stato di salute del paziente possano essere comunicate a soggetti diversi dal paziente stesso (genitori, tutore, amministratore di sostegno, prossimi congiunti, familiari, convivente, responsabile della struttura sanitaria).

All'interno di una struttura sanitaria complessa il personale incaricato di trattare dati sanitari è sicuramente vario e addetto a molteplici funzioni.

Non tutti questi incaricati sono afferenti a professioni sanitarie regolamentate, iscritti ad albi o ordini e pertanto soggetti al segreto che la loro professione richiede.

Per questo motivo, correttamente, il legislatore della privacy ha introdotto una norma di chiusura di carattere generale nella quale si dice che gli incaricati che all'interno di un organismo sanitario si trovino a trattare dati sanitari o a contenuto sanitario (si pensi agli addetti alle pulizie, al magazzino, ai pasti, alle attività segretariali) devono ugualmente considerarsi sottoposti ad un vincolo di segretezza analogo a quello delle professioni sanitarie che supportano e a regole di condotta similari, cui devono essere vincolati, se necessario, mediante apposite clausole nel loro contratto di lavoro[38].

9. Le misure di sicurezza tecnica. Le misure minime di sicurezza

Un corretto trattamento di dati sanitari richiede, data la delicatezza del loro contenuto, l'adozione di misure di sicurezza di carattere tecnico.

Le misure di sicurezza previste dal Codice privacy vengono distinte in misure *minime* di sicurezza e misure di sicurezza *idonee e preventive*.

Le misure minime di sicurezza sono previste nel Capo II del Titolo V e la loro mancata adozione è penalmente sanzionata.

Tali misure sono introdotte dall'art. 33 e meglio specificate negli articoli 34 e 35, mentre le modalità operative sono contenute nel disciplinare tecnico di cui all'Allegato B.

[38] Si veda l'articolo 83 comma 2 lettera i.

L'art. 34 si occupa del trattamento dei dati con strumenti elettronici (meglio: informatici) e prevede l'adozione delle seguenti misure minime:

a) l'autenticazione informatica[39];
b) l'adozione di procedure di gestione delle credenziali di autenticazione[40];
c) l'utilizzazione di un sistema di autorizzazione[41];
d) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici;
f) l'adozione di procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi;
g) la tenuta di un aggiornato documento programmatico sulla sicurezza[42];
h) *l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari*.

L'art. 35 è dedicato, invece, ai trattamenti che avvengano "senza l'ausilio di strumenti elettronici" e cioè essenzialmente, ai trattamenti che avvengano mediante documenti cartacei.

Il trattamento di dati personali effettuato *senza l'ausilio di strumenti elettronici* e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

[39] Definita dall'art. 4 del Codice come "l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità".

[40] Sono "credenziali di autenticazione" i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

[41] Inteso come l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

[42] Questa lettera è stata soppressa dal cosiddetto "Decreto Monti" per la semplificazione, più specificamente dall'art. 45, comma 1, lett.c), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

b) la previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) la previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il Disciplinare tecnico di cui all'Allegato B spiega e precisa quanto contenuto nell'art. 34. In particolare, con riferimento alle credenziali di autenticazione viene detto che esse consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata, conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, o infine in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o ad una parola chiave.

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi.

In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave va modificata almeno ogni tre mesi.

Dal Disciplinare tecnico è, inoltre, prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Quando, poi, per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un apposito sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

I dati personali oggetto di trattamento svolto con strumenti elettronici devono essere protetti contro il rischio di intrusione illecita, nonché contro l'azione

di programmi di cui all'art. 615-quinquies del codice penale[43], mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati almeno annualmente.

In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Dovranno essere impartite istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale.

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati dovranno essere distrutti o resi inutilizzabili, ovvero potranno essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Per quanto riguarda specificamente gli organismi sanitari e gli esercenti le professioni sanitarie, *questi dovranno effettuare il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.*

10. Le misure di sicurezza tecnica. Le misure di sicurezza idonee e preventive

Descritte le misure minime di sicurezza, la cui adozione, come si diceva, è obbligatoria e penalmente sanzionata, vanno poi prese in considerazione le misure di sicurezza cosiddette "idonee e preventive" introdotte, in termini generali, dall'art. 31.

[43] Si tratta della norma rubricata "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico" introdotta dalla legge 547 del 1993 a tutela dei programmi dagli attacchi dei cosiddetti "virus" nell'ambito delle modifiche al codice penale dirette a frenare il fenomeno dei cosiddetti "*computer crimes*".

Con riferimento ad esse il legislatore dice: "I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso o di trattamento non consentito o non conforme alle finalità della raccolta".

Le misure idonee e preventive non vengono quindi esplicitamente definite ed elencate, ma vengono enucleate in una clausola di tipo generale.

La scelta di tecnica legislativa è dovuta al fatto che il legislatore del Codice è consapevole che le tecnologie informatiche e telematiche sono soggette a rapida obsolescenza e a continuo progresso, per cui sarà responsabilità del titolare dei dati scegliere ed adottare le misure che di volta in volta gli appaiano migliori e più consone allo scopo, in rapporto allo stato della tecnica.

A differenza delle misure minime di sicurezza, la cui mancata adozione è reato, la mancata adozione delle misure idonee e preventive determina una responsabilità di tipo civile.

Al di là della evoluzione tecnologica, si deve ritenere, comunque, obbligata l'adozione di software antivirus e di meccanismi di *back up*, ma anche di sistemi anti-incendio e di allarme nei locali dove sono custoditi i dati.

11. La costruzione di una banca dati a contenuto sanitario

Gli organismi sanitari e i professionisti del settore, nel momento in cui intendono trattare i dati dei loro pazienti con l'ausilio dell'informatica e della telematica, si trovano inevitabilmente a dover creare delle banche dati contenenti informazioni sanitarie.

La creazione di *data base* sanitari è un'operazione molto delicata sotto il profilo del rispetto della normativa privacy e va posta grandissima attenzione sotto il profilo tecnico.

Il Codice si occupa più volte della questione: sintomo della grande importanza che il legislatore vi attribuisce.

Innanzitutto va esaminato l'art. 22, il cui 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".

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".

Queste precauzioni sono ribadite nella parte dedicata alle misure minime di sicurezza, la cui mancata adozione è, come si è detto, penalmente sanzionata.

Infatti l'art. 34, relativo, come si ricorderà, ai "Trattamenti con strumenti elettronici" 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 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 è proprio intenzionato a farlo il sanitario potrà vedere a chi si riferiscono quelle informazioni sanitarie e 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, 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 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*".

La realizzazione in termini tecnici delle indicazioni del legislatore sembra, dunque, 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.

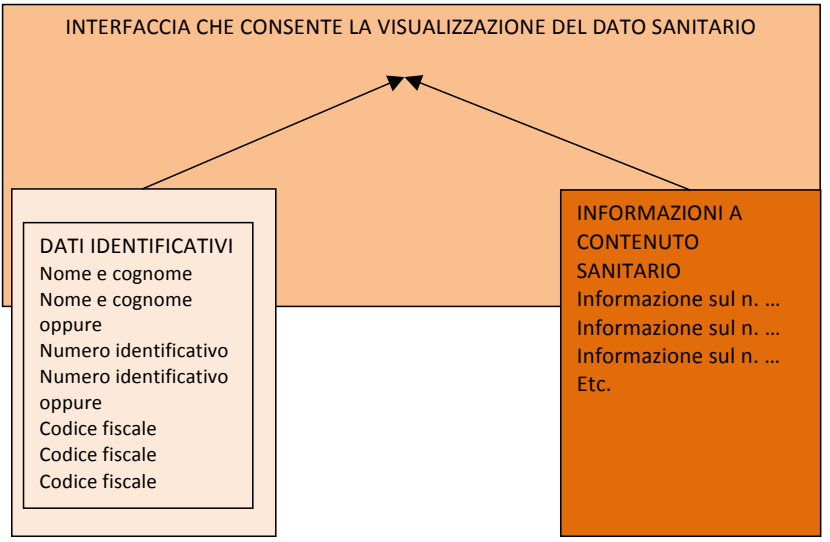
I dati identificativi potranno essere cifrati a livello di database tramite tecniche avanzate di crittografia: ciò consentirà di mantenere anonimi i dati idonei a rilevare lo stato di salute in caso di accessi non autorizzati al database.

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, 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.

La riunificazione 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.

Nella figura che segue cerchiamo di rappresentare graficamente il meccanismo ora descritto.



CAPITOLO TERZO

LA DOCUMENTAZIONE SANITARIA

1. Le cartelle cliniche

Il Codice della privacy introduce anche alcune indicazioni con riferimento alla redazione delle cartelle cliniche, affinché questo documento sanitario sia il più possibile rispettoso della privacy del paziente e di quella dei suoi familiari.

L'art. 92 al primo comma richiede, infatti, che la cartella clinica sia redatta in modo il più possibile chiaro e che i dati sanitari del paziente siano distinti da quelli relativi ai suoi familiari (raccolti evidentemente a fini di anamnesi).

Vi si dice in particolare: "nei casi in cui gli organismi sanitari pubblici e privati redigono e conservano una cartella clinica (…) devono essere adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati concernenti il paziente da quelli riguardanti altri interessati".

Con questa norma il legislatore si prefigge di proteggere il più possibile la riservatezza degli interessati i cui dati compaiono nella cartella.

Come è noto, infatti, è possibile, per varie ragioni, accedere alla cartella clinica anche se non si è il paziente a cui la cartella clinica si riferisce o il suo medico curante.

Uno dei motivi principali è quello di difendere in giudizio le proprie ragioni.

Con la soluzione organizzativa consistente nel raccomandare la massima comprensibilità possibile e nel distinguere, all'interno della cartella, i dati relativi al paziente dai dati relativi ai familiari, il legislatore si prefigge di evitare intrusioni immotivate dei terzi che legittimamente accedono alla cartella nei dati che non siano di loro interesse (in particolare con riguardo ai dati dei familiari).

La richiesta di accesso dovrà quindi essere motivata e avere un contenuto preciso.

Le autorità sanitarie si regoleranno di conseguenza, mostrando al richiedente solo i dati per i quali ha fatto la richieste e per cui è autorizzato all'accesso.

Quanto sopra trova conferma in una pronuncia del Garante secondo la quale l'amministrazione sanitaria, una volta che abbia ritenuto sussistente il diritto d'accesso alla documentazione contenente i dati sanitari, dovrà effettuare un'accurata selezione delle informazioni da rendere conoscibili ai richiedenti.

Ai sensi del secondo comma dell'art. 92, la richiesta di accesso alle cartelle cliniche da parte di soggetti terzi potrà essere accolta solo nei seguenti casi:

- necessità di far valere o difendere un diritto in sede giudiziaria, che sia di rango equiparabile al diritto alla riservatezza dell'interessato, o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile,
- necessità di tutelare una situazione giuridicamente rilevante di rango pari a quello dell'interessato, o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile.

La tutela della privacy in ambito sanitario si ottiene quindi anche grazie ad una adeguata predisposizione e gestione della vasta e varia documentazione impiegata dagli organismi sanitari e dagli esercenti le professioni sanitarie nel corso della loro attività.

Il principale di questi documenti è sicuramente la cartella clinica di impiego ospedaliero[44], che come si è visto, è espressamente menzionata dal Codice privacy.

Tuttavia vi sono anche altri documenti o insiemi di informazioni strutturate (referti, schede sanitarie, fascicoli sanitari elettronici, dossier sanitari) che sono molto importanti per l'attività sanitaria e che quindi vanno necessariamente presi in considerazione anche sotto il profilo della privacy.

È innanzitutto importantissimo ricostruire l'insieme delle norme in vigore nel nostro ordinamento che regolamentano tali documenti per poter comprendere le criticità che essi possono presentare sotto il profilo della tutela dei dati, specie nel caso di una loro redazione come documenti digitali.

Partiamo dalla già menzionata cartella clinica.

[44] Vedremo più avanti come l'insieme delle informazioni relative al paziente nel caso del medico di medicina generale non va indicato a rigori con l'espressione di "cartella clinica" ma con quella di "scheda sanitaria" e come i due documenti siano caratterizzati da natura giuridica e disciplina completamente diverse.

Non abbiamo nessuna norma che definisca con precisione cosa si deve intendere con "cartella clinica". Per questo motivo sono stati gli studiosi che si sono sforzati di stabilire cosa giuridicamente debba intendersi con essa.

La definizione che ne dà la dottrina è quella secondo cui "cartella clinica" si intende un documento che include sia le informazioni sulle condizioni cliniche del paziente connesse ai motivi del ricovero, sia indicazioni sulle situazioni pregresse e che vi possono poi essere registrati anche dati relativi ad altri soggetti, in particolare nel caso delle anamnesi familiari.

Ma qual è il valore giuridico di questi documenti?

Su questo punto la nostra Cassazione pare non avere più dubbi: le cartelle cliniche hanno valore probatorio di atto pubblico[45].

Si tratta, dunque, di un documento molto particolare, collocato dalla giurisprudenza della Cassazione proprio ai vertici della ideale graduatoria di documenti previsti dal nostro ordinamento.

Ed è considerata tale in quanto, chi redige e firma una cartella clinica attesta la verità di quanto ha scritto e firmato con lo stesso potere di certificazione dell'autorità sanitaria e in vece di questa.

Inoltre, per allargare il nostro ambito di indagine, va sottolineato come secondo la giurisprudenza della Cassazione sono atti pubblici anche il referto clinico (Cass. Pen. 10609/82), il certificato sanitario medico USL (Cass. Pen. 2207/1995) e una serie di certificati quali il certificato di morte (Cass. Pen. 181708/1989), il certificato di sana e robusta costituzione (Cass. Pen. 199666/1994), i certificati che attestano l'invalidità civile (Cass. Pen. 1004/2000) e il certificato di gravidanza[46].

[45] Si legga, in particolare, la sentenza della Cassazione Penale a Sezioni Unite dell'11 luglio 1992, n. 191175, ai sensi della quale la cartella clinica ha natura di atto pubblico in quanto "esplicazione di potere certificativo e partecipe della natura pubblica dell'attività sanitaria". Nel caso di specie, peraltro, viene riconosciuta natura di atto pubblico tanto in capo alla cartella clinica tenuta da una struttura pubblica ospedaliera quanto quella di una casa di cura convenzionata con il Servizio Sanitario Nazionale. Nello stesso senso del riconoscimento della natura di atto pubblico alla cartella clinica anche si vedano anche: Cassazione Penale Sez. V 193800/92; Cassazione Penale Sezione V 209682/97; Cassazione Penale Sezione V 184221/90.

[46] Si legga anche la nota e recente sentenza 35836 del 2007, frutto di un pronunciamento della Sesta Sezione Penale della Cassazione, la quale ribadisce la natura di pubblico ufficiale in capo al medico convenzionato in quanto nella sua attività estrinseca "poteri pubblicistici di certificazione".

Il riconoscimento operato dalla Cassazione di questi documenti come atti pubblici è stato principalmente effettuato al fine della applicazione di due articoli del Codice penale: l'articolo 476 e l'articolo 479, che si occupano, rispettivamente, del reato di falsità materiale e di falsità ideologica in atto pubblico.

In particolare, l'articolo 476, che si occupa del reato di falsità materiale, recita: "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni".

L'articolo 479, con riguardo alla falsità ideologica, prevede: "Il pubblico ufficiale che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476".

Ora, quando si è trattato di applicare la norma e di decidere nella pratica quali fossero gli atti pubblici ai fini dell'applicazione di questi articoli, la Cassazione penale ha indicato tra essi anche la cartella clinica, il referto e il certificato medico.

Si tratta di una presa di posizione univoca e coerente nel tempo della nostra giurisprudenza di legittimità da non trascurare.

L'atto pubblico, nel nostro ordinamento, ha anche una definizione in ambito civilistico. È definito infatti dall'art. 2699 del codice civile come "il documento redatto, con le richieste formalità, da un notaio o da un altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è stato formato".

Il rapporto tra l'atto pubblico in senso civilistico e l'atto pubblico in ambito penale è stato spiegato dalla stessa Cassazione, in particolare nella sentenza delle Sezione Unite n. 15983 dell'11 aprile 2006, relativa ai criteri per individuare l'atto pubblico. Nel caso specifico si trattava di valutare il valore giuridico del cartellino marcatempo utilizzato dai dipendenti della Pubblica Amministrazione.

Nella suddetta sentenza i giudici di legittimità hanno evidenziato come, secondo la costante giurisprudenza della Cassazione e la prevalente dottrina,

"agli effetti delle norme sul falso documentale, il concetto di atto pubblico è più ampio rispetto a quello che si desume dalla definizione contenuta nell'art. 2699 cod. civ., in quanto comprende non soltanto quei documenti che sono redatti con le richieste formalità da un notaio o da un altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede, ma anche i documenti formati da un pubblico ufficiale o da un pubblico impiegato incaricato di pubblico servizio nell'esercizio delle sue funzioni, attestanti fatti da lui compiuti o avvenuti in sua presenza ed aventi attitudine ad assumere rilevanza giuridica".

In buona sostanza la Cassazione intende mettere in guardia coloro che per una mansione di rilevanza pubblica sono incaricati di redigere e firmare atti che attestano fatti cui l'ordinamento attribuisce valore giuridico: devono, questi documenti, essere considerati anch'essi atti pubblici e quindi tutelati dalle norme penali contro il falso ideologico e materiale, anche se non sono propriamente conformi alla definizione civilistica di atto pubblico.

L'operatore sanitario sarà dunque soggetto alle fattispecie penali relative alla falsità in atti a prescindere dal fatto che la documentazione da lui redatta e sottoscritta sia civilisticamente inquadrabile nella definizione di "atto pubblico".

Per essere soggetto alle norme penali è sufficiente che per sua propria funzione sia chiamato a redigere e sottoscrivere atti che la giurisprudenza penale e la dottrina tendenzialmente riconoscano quale "esplicazione del potere certificativo pubblico".

Un dato è indubbio: la cartella clinica, e con lei altri documento sanitari quali i referti e i certificati, non sono per il nostro diritto comuni documenti amministrativi, bensì documenti collocati dal legislatore, per la rilevanza del loro contenuto e per l'espressione del potere di attestazione che consentono, ai vertici della gerarchia delle produzioni documentali previste dall'ordinamento.

2. Il Fascicolo Sanitario Elettronico. Le Linee Guida del Garante

Affrontiamo ora la trattazione del Fascicolo Sanitario Elettronico.

Non si tratta in questo caso di un vero e proprio documento utilizzato in ambito sanitario, ma piuttosto di un insieme strutturato di informazioni in modalità digitale, che possono includere anche dei documenti sanitari.

Il Fascicolo Sanitario Elettronico è stato per la prima volta previsto e disciplinato nel 2011 dal disegno di legge Fazio sulla riforma delle professioni sanitarie, senza divenire però norma di legge.

È stato poi nuovamente incluso, senza grandi modifiche rispetto alla disciplina contenuta nel disegno di legge Fazio, in un disegno di riforma della Sanità durante il Governo Monti, quello del Ministro della Salute Balduzzi, che lo ha presentato al Consiglio dei Ministri alla fine dell'estate del 2012.

Prima del disegno di legge Fazio, si erano già espressi in materia di Fascicolo Sanitario Elettronico sia il Ministero della Salute che l'Autorità Garante per la privacy.

Molto opportunamente, l'Autorità Garante per la protezione dei dati personali, rilevata "l'esigenza di individuare misure e accorgimenti necessari e opportuni da porre a garanzia dei cittadini interessati", ha avviato nel marzo 2009 una consultazione pubblica relativa al Fascicolo sanitario elettronico e al dossier sanitario, consultazione rivolta a tutti i soggetti e le categorie interessate, in particolare sottoposta all'attenzione "degli organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, degli organismi rappresentativi di operatori sanitari e delle associazioni di pazienti interessati".

Pertanto, il provvedimento contenente le Linee guida, originariamente adottato dall'Autorità il 22 gennaio 2009 e poi sottoposto a pubblica consultazione al fine di acquisire riscontri e osservazioni da far pervenire all'Autorità entro il 31 maggio, ha poi portato alla deliberazione in via definitiva delle "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario" in data 16 luglio 2009.

In esse il Garante per la privacy precisa che sia il fascicolo che il dossier si collocano nell'ambito del "processo di ammodernamento della sanità pubblica e privata"e che si prefiggono di "migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure".

Il contributo dato in questa sede dall'Autorità garante risulta di grande rilevanza nell'ottica di sgombrare primariamente il campo da questioni terminologiche e funzionali.

Dalle indicazioni del Garante risulta chiaro come il FSE non debba essere confuso con la cartella clinica (elettronica o meno) che, per riconoscimento dello stesso Garante, è oggetto di una sua propria disciplina giuridica[47].

Né va commesso l'errore di confondere il contenuto del futuro FSE con l'insieme delle informazioni che il medico di medicina generale raccoglie sulla salute del proprio paziente nella scheda sanitaria, documento per ora ad uso esclusivamente interno del medico di famiglia.

Del FSE il Garante dà una prima descrizione, secondo la quale si tratta di un "fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale".

Da tale definizione si desume la natura del FSE come un insieme coordinato e funzionale di informazioni di varia provenienza attinenti allo stato di salute del cittadino/paziente, finalizzate alla sua cura.

In questa prima descrizione non si fa menzione di documenti sanitari: stando a questa definizione potrebbe trattarsi solo di un insieme di dati e informazioni, raccolte in modo logico e razionale per la cura del cittadino.

Tuttavia, nel prosieguo delle citate Linee guida, ci si sofferma sul fatto che "nel caso di FSE" vengono "in considerazione documenti sanitari del tutto distinti tra loro" e infine, nel paragrafo rubricato "Comunicazioni al Garante" se ne dà la seguente definizione: "un insieme logico di informazioni e *documenti sanitar*i volto a documentare la storia clinica di un individuo condiviso da più titolari del trattamento".

La natura del Fascicolo Sanitario Elettronico come di un insieme di documenti sanitari richiede particolare cura e attenzione sotto il profilo giuridico e della privacy, in quanto, come si è visto a proposito della caratteristica di atto pubblico della cartella clinica, del referto e dei certificati, molto documenti sanitari hanno una loro "storia giuridica" e un loro inquadramento normativo, dottrinario e giurisprudenziale, di cui bisogna tenere conto in sede di realizzazione del FSE e di digitalizzazione di questi documenti, tradizionalmente cartacei.

[47] Come trattato nel precedente paragrafo, la cartella clinica – di genesi ospedaliera - per costante giurisprudenza della Cassazione è un atto pubblico e gode inoltre di apposita regolamentazione per quanto concerne la sua archiviazione conservazione.

Un elemento su cui riflettere è esemplificativamente il fatto che il FSE sarà il fascicolo informatico che conterrà, una volta implementato, l'insieme più numeroso e vario di documenti che sono atti pubblici, almeno sotto il profilo penalistico, rispetto a tutti i fascicoli digitali finora normativamente previsti nell'ambito della Pubblica Amministrazione.

Una vera rivoluzione.

Per la stessa natura di "atto pubblico" di alcune delle entità documentali contenute, alla suddette "informazioni organizzate" non potranno essere applicate automaticamente le norme del Codice dell'Amministrazione Digitale previste per i documenti informatici e per i documenti informatici amministrativi, trattandosi nel caso di specie di un atti amministrativi informatici molto particolari, ovvero di "atti pubblici informatizzati".

La redazione di tali atti pubblici comporta che, in questi casi, la firma (nel caso di documenti in formato digitale si tratterà della firma digitale) viene apposta nel documento sanitario eventualmente informatizzato non semplicemente da un medico o altro operatore sanitario, ma da un medico in veste di pubblico ufficiale.

In base alle Linee guida, scopo del "Fascicolo sanitario elettronico" e "Dossier sanitario" saranno "la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica".

Alla luce della funzione attribuita a tali strumenti, il Garante arriva quindi alla conclusione che "il FSE e il dossier" conterranno "diverse informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica" e che i suoi dati personali saranno "collegati tra loro con modalità informatiche di vario tipo che ne rendono, comunque, possibile un'agevole consultazione unitaria da parte dei diversi professionisti o organismi sanitari che prendono nel tempo in cura l'interessato".

Si parla di dossier sanitario "qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti".

Si intende invece per FSE il "fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta)".

In considerazione del fatto che il FSE non aveva (e non ha) ancora trovato un suo riconoscimento normativo, l'Autorità Garante riteneva opportuno intervenire a tutela della privacy del paziente in questo ambito ancora pionieristico e deregolamentato.

Ad ogni buon conto, per quanto non abbiano il valore di norma di legge in quanto promananti da un'Autorità indipendente, è opportuno tenere conto delle raccomandazioni del Garante in merito alla realizzazione e gestione del FSE:

Innanzitutto, poiché i dati sanitari e i documenti che faranno parte del FSE proverranno da più soggetti diversi, dovranno essere adottati idonei procedimenti informatici che consentano di individuare la fonte di provenienza di ciascun dato: quale organismo o professionista cioè lo ha raccolto, prodotto e chi lo ha reso accessibile.

In tal modo sarà possibile comporre e mantenere un quadro chiaro di responsabilità con riguardo al trattamento dei dati contenuti, in quanto il soggetto che ha prodotto e inserito i dati ne manterrà di regola la titolarità e le conseguenti responsabilità giuridiche civili e penali.

Con riguardo alle finalità del trattamento dei dati, tale trattamento, secondo il Garante, dovrà essere incentrato nelle attività di cura, diagnosi e prevenzione a vantaggio del paziente.

Il Garante aggiunge però che "qualora attraverso il FSE o il dossier si intendano perseguire anche talune finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria richiesta dall'interessato (es. prenotazione e pagamento di una prestazione), tali strumenti dovranno essere strutturati in modo tale che i dati amministrativi siano separati dalle informazioni sanitarie, prevedendo profili diversi di abilitazione degli aventi

accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite".

Inoltre "eventuali, future utilizzazioni anche parziali del FSE o del dossier per ulteriori fini di ricerca scientifica, epidemiologica o statistica" non saranno di per sé precluse, ma potranno verificarsi solo in conformità alla normativa di settore e dovranno essere oggetto di preventiva e specifica attenzione.

3. Il Fascicolo Sanitario Elettronico. Il riconoscimento del principio di autodeterminazione

La questione maggiormente dibattuta in relazione alla progettazione FSE è quella che riguarda il suo contenuto: quali siano cioè i dati sanitari che potranno lecitamente confluire nel fascicolo e quale dovrà essere il grado di incidenza della volontà del paziente su tale contenuto.

Si tratta di aspetti fondamentali che sono già stati oggetto dell'attenzione dei Garanti europei in sede di elaborazione delle Linee guida sulla cartella clinica elettronica (CCE)[48].

In proposito, il Gruppo dei garanti europei già riconosceva l'importanza del principio di "autodeterminazione del paziente", in relazione al quale si affermava che "la decisione del paziente sul come e il quando usare i suoi dati deve rivestire un ruolo fondamentale come garanzia importante".

Il riconoscimento del principio di autodeterminazione da parte del paziente non era tuttavia visto come assoluto dai Garanti europei, i quali, nel citato documento, affermavano che "un sistema di CCE non è interamente fondato sul consenso come base giuridica" e aggiungevano che "poiché i diversi tipi di dati sulla salute non hanno lo stesso potenziale di arrecare pregiudizio, andrebbero distinte delle categorie di utilizzo con vari gradi di possibilità d'esercizio dell'autodeterminazione".

[48] Si legga in proposito il "Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)", adottato il 15 febbraio 2007. Il gruppo di lavoro, istituito ai sensi dell'articolo 29 della direttiva 95/46/CE, è un organo europeo indipendente a carattere consultivo in materia di protezione dei dati e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

In Italia il tema è stato oggetto di acceso dibattito e l'Autorità garante per la privacy nelle citate Linee guida per il Fascicolo Sanitario Elettronico, prende decisamente posizione a favore dell'autodeterminazione del paziente.

Il Garante della privacy si raccomanda che sia consentito al paziente di "scegliere, in piena libertà, se far costituire o meno un Fse/dossier con le informazioni sanitarie che lo riguardano".

Altrimenti deve essere garantita al paziente la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti.

Non solo: non si tratta di garantire la autodeterminazione solo con riguardo al "se" far redigere un proprio FSE, ma anche sul "come" tale fascicolo debba essere costituito.

Il nostro Garante arriva infatti ad affermare che il paziente deve potersi liberamente esprimere su quali informazioni egli vuole che siano inserite nel fascicolo e deve essere possibile che alcune informazioni sanitarie che lo riguardano non siano menzionate affatto nel fascicolo.

Quindi alcune notizie molto importanti sul paziente potrebbero non comparire nel suo fascicolo, se egli lo vuole. Si tratta del cosiddetto "oscuramento" del FSE.

Ma non basta. Il Garante richiede che gli operatori sanitari che consultano il fascicolo non siano neppure in grado di accorgersi che l'interessato ha deciso di oscurare una determinata informazione. Per intenderci: supponiamo che il paziente sia celiaco e che non voglia che questa informazione sia resa nota mediante il suo FSE. Egli può evitare di inserirla. Ma non ci deve essere all'interno del suo FSE nessun "indizio" da cui il medico possa desumere che non ha voluto metterla.

Per esemplificare in modo molto banale, non ci deve essere una frase "il paziente è celiaco" e due caselle "sì" e "no" che il medico possa compilare, perché se il medico non le compilasse né con un sì né con un no, chi legge il fascicolo si accorgerebbe che il paziente non ha voluto pronunciarsi circa il fatto di essere o meno celiaco.

Quindi, l'oscuramento dovrebbe avvenire in modo tale da far sì che gli operatori sanitari non siano in grado di venire a conoscenza del fatto che esso si è verificato (cosiddetto "oscuramento dell'oscuramento").

Come si è detto, la posizione del Gruppo ex articolo 29 sarebbe più moderata: si suggerisce di distinguere "diversi tipi di dati sulla salute" in rapporto alla loro potenzialità di arrecare danno alla privacy del paziente e di "creare diversi moduli di dati con diverse condizioni di accesso".

Per esempio, un modulo di dati "vaccinazioni" oppure "allergie" o "intolleranze ai farmaci" dovrebbero essere accessibili in ogni momento alla persona interessata e potrebbero anche esserlo per un numero piuttosto ampio di operatori sanitari; un modulo "emergenze" potrebbe prevedere mezzi tecnici speciali per l'accesso.

Nello senso della possibilità di un temperamento funzionale del principio di oscuramento si pone anche il Garante italiano nelle citate Linee guida nel momento in cui dà atto che "in alcuni progetti esaminati all'interno del Fse/dossier è stata poi individuata una sintesi di rilevanti dati clinici sul paziente, ovvero un insieme di informazioni la cui conoscenza può rivelarsi indispensabile per salvaguardare la vita dell'interessato (es., malattie croniche, reazioni allergiche, uso di dispositivi o farmaci salvavita, informazioni relative all'impiego di protesi o a trapianti). Tali informazioni – raccolte di regola in un modulo distinto - sono conoscibili da parte di tutti i soggetti che prendono in cura l'interessato".

4. Il Fascicolo Sanitario Elettronico. Le Linee Guida ministeriali

Alle Linee guida del Garante privacy sono seguite, nel novembre 2010, le Linee guida del Ministero della Salute.

Esse definiscono il FSE come un "insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, che ha come scopo principale quello di agevolare l'assistenza al paziente, offrire un servizio che può facilitare l'integrazione delle diverse competenze professionali, fornire una base informativa consistente, contribuendo al miglioramento di tutte le attività assistenziali e di cura, nel rispetto delle normative per la protezione dei dati personali".

La definizione ministeriale include quindi pacificamente i documenti digitali di tipo sanitario all'interno del FSE, nel quale quindi ci aspetteremo di trovare cartelle cliniche, referti e certificati.

Per altro verso, tale definizione, sicuramente per motivi di missione istituzionale dell'organo emanante, pare meno incentrata di quella del Garante sulla salute e sulla cura del paziente e maggiormente sulla predisposizione di tutto l'apparato assistenziale e burocratico necessario per tale attività di cura.

La finalità del trattamento del dato sanitario sembra pertanto essere, nella visione del ministero, volta alla cura del paziente solo in via mediata, mentre in via immediata, e per la natura stessa dell'organo che ha predisposto queste Linee guida, l'approccio ministeriale pare più concentrato sugli aspetti amministrativi, gestionali e di controllo di spesa.

Le Linee guida ministeriali introducono poi un oggetto documentale nuovo: il cosiddetto *Patient Summary* (o Profilo Sanitario Sintetico).

Si dovrebbe trattare di un documento di importanza cruciale, dato il suo ruolo di "riassunto della storia clinica del paziente e della sua situazione corrente".

La redazione e la tenuta di tale documento è affidata dalle Linee guida al medico di medicina generale. Esse infatti affermano: il *Patient Summary* "è creato, aggiornato e mantenuto solo dal MMG/PLS; non può essere creato in maniera automatica a partire dal FSE; è sempre frutto di una valutazione professionale e la frequenza di aggiornamento, che deve essere adeguata, è a discrezione del MMG/PLS".

Al medico di medicina generale viene quindi affidata una rilevante responsabilità: quella della creazione, del mantenimento e dell'aggiornamento del riassunto della storia clinica del paziente.

Con riguardo poi al rapporto tra le indicazioni contenute nelle Linee guida ministeriali e le raccomandazioni del Garante privacy, si riscontra una piena adesione – per lo meno formale - nelle Linee guida del ministero della Salute, alle osservazioni dell'Autorità Garante.

Si legge nelle indicazioni ministeriali: "Il trattamento dei dati personali del FSE deve rispettare pienamente le norme che disciplinano la protezione di tali dati e deve pertanto assoggettarsi alla libera volontà dell'assistito, che con il proprio consenso ha facoltà di permettere o meno la costituzione del proprio FSE, di far confluire in esso i dati relativi al suo stato di salute pregresso e/o attuale e di esercitare il potere di controllo su chi può accedere al proprio

fascicolo e a quali gruppi di informazioni. Le sue scelte possono essere da lui modificate in qualsiasi momento".

Il Ministero aderisce inoltre completamente alla posizione del Garante circa l'opportunità dell' "oscuramento" nonché dell' "oscuramento dell'oscuramento": "Ulteriore garanzia per l'assistito è la facoltà di non consentire la visibilità di alcune informazioni sanitarie relative a singoli eventi clinici, che potrebbero andare a confluire nel FSE, a soggetti diversi da chi ha prodotto il dato (oscuramento) senza che quest'ultimi vengano automaticamente a conoscenza del fatto che l'assistito abbia effettuato tale scelta ("oscuramento dell'oscuramento")".

La natura del FSE come emerge dalle indicazioni ministeriali è - a parere di chi scrive - minata da una forte ambiguità: da un lato il suo contenuto ne è dettagliatamente descritto (dati identificativi e dati amministrativi del paziente, nucleo minimo ed essenziale dei dati sanitari, altri documenti, tra cui in particolare il *Patient summary*).

Dall'altro però tutto il suo prezioso contenuto, delineato minuziosamente nelle Linee guida ministeriali, risulta "minacciato" da una applicazione non solo teorica ma reale ed effettiva dal principio dell'oscuramento.

Il Ministero ci dice infatti nella prima parte delle Linee guida cosa esattamente potrà trovarsi nel FSE, ma poi "si scopre" nella seconda parte dello stesso regolamento che in un FSE "reale" potrebbe non esservi nulla o quasi, avendo il paziente esercitato il suo diritto all'oscuramento.

O addirittura che il paziente potrebbe non avere un FSE ("*Il consenso alla creazione del proprio Fascicolo sanitario elettronico, da parte dell'assistito, deve essere esplicito*", cioè manifestato inequivocabilmente, quindi non intuito o desunto da un comportamento, non soddisfacendo il criterio del carattere "esplicito" la soluzione del silenzio-assenso (opt-out)"). Con buona pace della responsabilità del medico di medicina generale, cui potrebbe essere affidata la manutenzione e l'aggiornamento di una "scatola vuota".

Quelle sopra descritte sono le perplessità giuridiche di maggiore rilevanza. Ma non sono le sole. Vale la pena anche di riflettere sulla natura e sul valore giuridico del cosiddetto "Taccuino personale del cittadino".

Ci dicono le Linee guida: "Nell'ambito del FSE si può prevedere una sezione riservata al cittadino per offrirgli la possibilità di inserire dati ed informa-

zioni personali (es. dati relativi al nucleo familiare, dati sull'attività sportiva, ecc.), file di documenti sanitari (es. referti di esami effettuati in strutture non convenzionate, referti archiviati in casa), un diario degli eventi rilevanti (visite, esami diagnostici, misure dei parametri di monitoraggio), promemoria per i controlli medici periodici. Questo consente di arricchire il FSE con ulteriori informazioni al fine di completare la descrizione dello stato di salute, ma tali informazioni e/o documenti risulteranno "non certificate"".

Quale attenzione dovrà prestare l'operatore sanitario al contenuto di tale "taccuino personale" del suo paziente? Fino a che punto dovrà tenerne conto? Quale attendibilità o corrispondenza al vero dovrà il medico attribuire a informazioni e notizie inserite dal paziente ma "non certificate"? Ma soprattutto: quale responsabilità in giudizio gli sarà riconosciuta per averne (o non averne) tenuto conto? La questione è tuttora molto dibattuta.

5. Il Fascicolo Sanitario Elettronico. I disegni di legge Fazio e Balduzzi

Il percorso formativo del FSE include altre due tappe di rilievo: la presentazione alla Camera, il 7 aprile del 2011 di un disegno di legge da parte del Ministro della Salute Fazio riguardante "Sperimentazione clinica e riforma degli ordini delle professioni sanitarie" – durante il governo Berlusconi - e la presentazione di un decreto legge recante "Disposizioni urgenti per promuovere lo sviluppo del paese mediante un più alto livello di salute" – durante il governo Monti – da parte del Ministro della Salute Balduzzi[49].

Per quanto concerne il disegno di legge Fazio, il titolo III del disegno di legge era rubricato: "Sanità elettronica" e, in caso di approvazione della norma, sarebbe stata la prima volta che in un testo di legge che disciplina il nostro Servizio Sanitario Nazionale compariva l'espressione di "Sanità elettronica".

L'articolo 12 del citato titolo si occupava specificamente del Fascicolo elettronico: "Disposizioni in materia di fascicolo sanitario elettronico" e lo definiva

[49] Decreto legge *recante disposizioni urgenti per promuovere lo sviluppo del paese mediante un più alto livello di tutela della salute* del 10 agosto 2012, presentato alle Regioni il 24 agosto, all'approvazione del Consiglio dei Ministri il 31 agosto 2012. Il decreto legge è stato approvato dal Consiglio dei Ministri, ma le norme relative al Fascicolo Sanitario Elettronico ne sono state stralciate.

come "l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito". La definizione che ne veniva data non si discostava quindi da quella delle citate linee guida del Garante e del Ministero.

Sulla base della competenza in materia di sanità costituzionalmente affidata alle regioni, la sua istituzione era affidata a queste (e alle province autonome), ovviamente nel rispetto della normativa nazionale sul trattamento dei dati personali.

Le finalità del FSE indicate nel disegno di legge (e quindi le finalità per le quali mediante il FSE saranno trattati i dati a contenuto sanitario dei pazienti) sono molteplici e vanno ben al di là dello scopo di cura in senso stretto.

Si tratta di:

a) prevenzione, diagnosi, cura e riabilitazione;

b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;

c) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria.

Il comma terzo dell'articolo 12 prevedeva che il fascicolo sanitario fosse alimentato in maniera continuativa dai soggetti che prendono in cura l'assistito nell'ambito del Servizio sanitario nazionale e dei servizi socio-sanitari regionali.

Si deve ritenere che gli organismi sanitari e gli esercenti le professioni sanitarie che alimenteranno il FSE, già titolari dei dati che vi hanno immesso, ne manterranno la responsabilità giuridica anche una volta che questi siano stati digitalizzati e inseriti nel nuovo oggetto informatico, come raccomandato dalle Linee Guida del Garante privacy[50].

Come si diceva, al di là degli scopi tipici dell'attività sanitaria (prevenzione, diagnosi, cura e riabilitazione), si prevede l'impiego dei dati contenuti nel FSE

[50] Si legga in particolare la Parte I "Il Fascicolo sanitario elettronico e il dossier sanitario" al punto 2 "Ambito di applicazione delle Linee guida": "Nel caso di Fse, venendo poi in considerazione documenti sanitari del tutto distinti tra loro, *deve essere assicurato che ciascun soggetto che li ha prodotti autonomamente ne rimanga di regola l'unico titolare*, anche se le informazioni sono -come detto- disponibili agli altri soggetti abilitati all'accesso (ad esempio -come spesso accade-, attraverso la condivisione, da parte di tutti i soggetti che prendono in cura l'interessato, dell'elenco degli eventi sanitari occorsi, elenco strutturato anche sotto forma di indici o di puntatori logici dei singoli episodi clinici)".

anche per finalità di ricerca scientifica (lettera *b*) e per finalità di programmazione, gestione e controllo e valutazione dell'assistenza sanitaria (lettera *c*).

Quest'ultimo impiego dei dati sanitari dei pazienti è molto dibattuto in quanto ci si domanda fino a che punto per funzioni di programmazione e gestione sia necessario usare i dati personali dei pazienti, o se invece non siano sufficienti dati anonimi o aggregati.

Con riguardo a questa spinosa questione, l'art. 12 ai commi 5 e 6 così stabilisce: nel caso in cui il SSN persegua finalità di cura, per la consultazione dei dati del paziente all'interno del FSE è necessario il consenso del paziente, salvi i casi di emergenza sanitaria in cui il paziente non è in grado di darlo.

Nel caso invece in cui l'accesso ai dati del FSE avvenga da parte di regioni, province autonome e Ministero della Salute per finalità di ricerca e di gestione e controllo (lettere b e c), il perseguimento di tali finalità avverrà *senza l'utilizzo dei dati identificativi degli assistiti e dei documenti clinici presenti nel FSE* e *in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali*.

Pare quindi che il disegno di legge, nel caso di accesso a fini di ricerca scientifica e di controllo e gestione, miri alla massima tutela della privacy dell'assistito, laddove raccomanda di non utilizzare i dati identificativi degli assistiti e il rispetto dei principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali.

Tuttavia, all'interno del FSE il dato non si trova in forma anonima, ma deve essere reso tale dal suo utente, sia esso il Ministero o la regione: per questo motivo – ci sembra di intendere - il legislatore raccomanda massima cura e attenzione con riguardo alla fase di anonimizzazione e tempestività in questa operazione, proprio sulla base dei principi di proporzionalità e di necessità menzionati.

Le modalità di anonimizzazione del dato dovranno essere stabilite mediante un regolamento, che dovrà essere adottato entro sei mesi dalla data di entrata in vigore della presente legge, con decreto del Ministro della salute, di concerto con il Ministro dell'economia e delle finanze e con il Ministro per la pubblica amministrazione e l'innovazione.

Il citato regolamento stabilirà: i contenuti del FSE, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti

dell'assistito, le modalità e i livelli diversificati di accesso al FSE da parte del SSN, delle regioni e del Ministero.

Esso avrà quindi un peso rilevante nella effettiva regolamentazione del FSE.

Nello stesso comma 7 si prevede che tale decreto dovrà anche stabilire "le modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato".

Pur senza mettere in discussione l'utilità di tale codice identificativo, è bene che si rammenti che l'abbinamento dell'informazione sanitaria al dato identificativo del paziente non ne fa un dato anonimo, ma semplicemente un dato in cui l'interessato/paziente non è immediatamente identificato, ma è identificabile[51].

In questo caso quindi si ha ancora a che fare con dati personali sanitari e si rientra in pieno nell'applicazione del Codice della privacy: nulla a che fare con l'anonimato.

Il disegno di legge Fazio non ha raggiunto il vigore legislativo e, cessato il governo Berlusconi, il governo Monti ha nuovamente affrontato la questione mediante il decreto legge del Ministro della Salute Balduzzi.

Il testo del decreto legge sottoposto all'approvazione del Consiglio dei Ministri a fine agosto del 2012 riproponeva senza sostanziali modifiche il precedente disegno di legge. Il decreto legge è stato approvato, tuttavia gli articoli relativi al FSE ne sono stati stralciati, per cui la materia è tuttora deregolamentata.

La realizzazione del FSE potrà rappresentare uno strumento di grande utilità per la salute del cittadino, ma dovrà essere effettuata tenendo conto del principio di autodeterminazione del paziente e, di non minore importanza, della disciplina giuridica dei documenti e dei dati in esso contenuti.

La questione del regime giuridico del dato a contenuto sanitario diviene assolutamente di primaria importanza proprio in relazione alla progettazione del Fascicolo sanitario elettronico.

Un principio cardine di cui tenere conto e da cui dipende la liceità del trattamento del dato è il principio di necessità, in base al quale il dato personale va trattato solo qualora tale trattamento sia *assolutamente indispensabile* ai fini

[51] Quanto detto vale in particolare qualora il codice identificativo sia basato sul codice fiscale.

del perseguimento di una determinata finalità. In caso contrario, l'informazione va trattata in forma anonima[52].

Con specifico riguardo ai sistemi informativi, l'art. 3 comma 1 del Codice privacy prescrive inoltre: "I sistemi informativi e i programmi informatici sono configurati *riducendo al minimo l'utilizzazione di dati personali e di dati identificativi*, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

Ai fini pertanto della predisposizione di un quadro normativo e regolamentare corretto ed esaustivo che disciplini il Fascicolo sanitario elettronico, si ritiene che non si possa prescindere dalla *chiara ed inequivocabile indicazione delle finalità per cui ciascun tipo di dato a contenuto sanitario sarà trattato* (a tutela della salute del paziente, di terzi, della collettività, per fini amministrativi, per fini di ricerca, per fini statistici, per scopi commerciali), in quanto proprio la finalità - in base al principio di necessità - sarà criterio determinante per stabilire se tale trattamento è lecito o meno, se può essere eventualmente effettuato in termini anonimi e comunque quale ne debba essere la disciplina normativa.

6. Il referto on line

In analogia con quanto verificatosi con riferimento al FSE, nel 2009 l'Autorità garante per il trattamento dei dati personali ha adottato in via definitiva le "Linee guida in tema di referti on line[53]", al fine di regolamentare in modo conforme ai principi della privacy l'utilizzo dei referti digitalizzati e il loro invio o la loro consegna al paziente.

Anche in questo caso, anteriormente alla adozione del testo delle Linee Guida nella loro versione definitiva, il Garante ne ha redatto e pubblicato il testo[54] e

[52] Art. 11, comma 1 lett. d: "I dati personali oggetto di trattamento sono (…) non eccedenti rispetto alle finalità per i quali sono raccolti e successivamente trattati".

[53] Linee guida in tema di referti on-line, 19 novembre 2009, pubblicate in G.U. n. 288 dell'11 dicembre 2009.

[54] Il testo è stato adottato con provvedimento a carattere generale del Garante in data 25giugno 2009 e pubblicato in Gazzetta Ufficiale in data 15 luglio 2009, la n. 162.

lo ha sottoposto ad apposita consultazione pubblica, grazie alla quale ha potuto raccogliere osservazioni e commenti di organismi e professionisti sanitari pubblici e privati e di associazioni di pazienti interessati in tema di referti on line.

Innanzitutto il Garante precisa, nelle Linee Guida, che per "referto" deve intendersi "la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale".

Anche nel caso del referto on line, come in quello del FSE manca ancora una previsione e disciplina normativa e, parallelamente a quanto previsto in relazione alla formazione del Fascicolo sanitario elettronico, anche con riguardo ai referti digitali, a giudizio del Garante deve prevalere il diritto all'autodeterminazione del cittadino e di massima libertà decisionale dello stesso nella scelta della modalità di ricezione.

All'interessato, quindi, deve essere consentito di scegliere - in piena libertà - *se accedere o meno al servizio di refertazione on-line*.

In caso contrario e data l'assenza di qualsiasi previsione normativa in materia che vincoli il cittadino, *gli dovrebbe essere garantita la possibilità di continuare a ritirare i referti cartacei presso la struttura erogatrice della prestazione*.

La struttura sanitaria dovrà predisporre allo scopo una specifica informativa e dovrà effettuare la raccolta del relativo consenso in ordine al trattamento dei dati personali connessi a tale servizio, in modo da consentire al cittadino di aderire – qualora lo voglia -consapevolmente e con adeguato livello di informazione a tali servizi di refertazione, senza alcun pregiudizio circa la possibilità di usufruire comunque delle prestazioni mediche richieste.

Non solo, ma la libertà di scelta del cittadino, secondo il Garante, deve potersi esprimere fino al limite per cui, qualora l'interessato abbia scelto di aderire ai suddetti servizi di refertazione, deve essergli altresì concesso - in relazione ai singoli esami clinici a cui si sottoporrà di volta in volta - di manifestare una volontà contraria, nel senso di poter ricevere il referto in modalità diversa da quella originariamente opzionata.

Per intenderci: qualora il cittadino abbia scelto di ricevere i referti via mail, deve poter anche, nel caso in cui lo voglia, andare a ritirare il referto di persona, naturalmente previa debita comunicazione.

La messa a disposizione del cittadino dei referti in modalità digitale avviene generalmente attraverso due modalità: la ricezione del referto presso la casella

di posta elettronica dell'interessato oppure il collegamento al sito Internet della struttura sanitaria ove è stato eseguito l'esame clinico, al fine di effettuare il *download* del referto stesso.

In applicazione del principio di libera determinazione del cittadino, nel caso di comunicazione del referto presso l'indirizzo della casella di posta elettronica fornito dall'interessato, a quest'ultimo deve essere concessa la possibilità di confermare l'indirizzo di posta elettronica in cui ricevere tale comunicazione in occasione dei successivi accertamenti clinici.

Il cittadino, cioè, deve poter decidere di utilizzare un diverso indirizzo e-mail le volte successive e di volta in volta, qualora lo ritenga opportuno.

Il Garante, tuttavia, precisa in questa stessa sede che devono tenute ferme le norme che disciplinano la Posta Elettronica Certificata e dunque che "resta ferma l'operatività del sistema che verrà adottato ai sensi del d.P.C.M. 6 maggio 2009 in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini".

Interpretando la suddetta disposizione del Garante, si può quindi arrivare a supporre una progressiva qualificazione del sistema di Posta Elettronica Certificata quale canale preferenziale per l'invio la cittadino della sua refertazione digitale da parte delle strutture sanitarie.

Il cittadino, inoltre, deve poter scegliere, di volta in volta o anche *una tantum* – se ricevere via mail i referti clinici, anziché dalla struttura sanitaria che ha effettuato l'esame, dal proprio medico curante o dal proprio medico di medicina generale.

All'opposto devono anche essergli garantiti il diritto e la possibilità tecnica di non comunicare sistematicamente al medico curante tutti i risultati delle indagini cliniche effettuate, lasciandogli la possibilità di scegliere, di volta in volta, quali referti mettergli a disposizione.

Tornando alle modalità tecniche ordinarie di messa a disposizione del referto digitale, nel caso di scelta del sistema di *download*, al fine di effettuare la copia locale o la visualizzazione interattiva del referto, devono essere adottate delle specifiche cautele, data la tipologia del dato trattato.

In particolare:

- protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici, che prevedono la certificazione digitale dell'identità dei sistemi

che erogano il servizio in rete (per esempio il sistema *Secure Socket Layer* nell'ambito del protocollo *https* su *web*);
- tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel documento digitale nel caso di sua memorizzazione intermedia in sistemi di *caching*, locali o centralizzati, a seguito della sua consultazione on-line;
- l'utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di *strong authentication*;
- disponibilità al *download* limitata nel tempo (massimo 45 giorni), per ridurre i rischi di accesso abusivo;
- possibilità da parte dell'utente di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.

In caso di comunicazione per e-mail del referto, il Garante raccomanda:
- la spedizione del referto in forma di allegato a un messaggio e-mail e non nel formato di un testo compreso nella *body part* del messaggio;
- che il file contenente il referto sia protetto con modalità idonee a impedire l'illecita o accidentale acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati. Tali misure di sicurezza potranno consistere in una *password* per l'apertura del file o nell'impiego di un sistema di cifratura, in cui la password o la chiave crittografica siano rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti.

A parere del Garante, a fini di semplificazione, password e chiave crittografica potranno non essere adottate qualora l'interessato ne faccia espressa e consapevole richiesta, in quanto l'invio del referto alla casella di posta elettronica indicata dall'interessato "non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l'interessato effettuata su specifica richiesta di quest'ultimo".

Infine, si raccomanda la convalida degli indirizzi e-mail tramite apposita procedura di verifica on-line, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

È prevista, inoltre, nelle Linee guida l'utilizzazione del servizio di avviso via telefono cellulare tramite *short message service* (sms).

Nel messaggio, però, dovrà essere data solo notizia della disponibilità del referto e non ovviamente anche del dettaglio della tipologia di accertamenti effettuati, del loro esito o delle credenziali di autenticazione assegnate all'interessato: l'invio di ogni altra informazione, infatti, potrebbe creare criticità con riferimento sia alla tutela della privacy dell'assistito sia con riferimento alla difficoltà di organizzare correttamente e con chiarezza l'informazione medica all'interno di uno sms.

Circa gli obblighi di informativa e consenso, ai fini dell'invio del referto *dovrà essere fornita idonea informativa*, distinta da quella resa per finalità di cura; dopo aver fornito l'informativa, opportunamente il Garante prevede che la struttura sanitaria acquisisca un *autonomo specifico consenso*.

Inoltre, in applicazione del generale principio di oblio, *dovrà essere garantita al cittadino la possibilità di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema* di consultazione, in modo complessivo o selettivo, *i referti che lo riguardano*.

Il descritto intervento del Garante a tutela dei dati sanitari del cittadino nel caso di utilizzo di referti digitali è sicuramente opportuno e meritevole, ma – come lo stesso Garante riconosce – essi non sono ancora stati regolamentati dal legislatore nazionale.

Quando il legislatore se ne occuperà, dovrà farlo, a nostro giudizio, tenendo conto del valore giuridico e dell'efficacia probatoria in giudizio del referto (fino a poco tempo fa solo cartaceo, ma già latore di proprie prerogative giuridiche), e quindi considerando non solo gli aspetti privacy, ma anche il fatto che il referto costituisce estrinsecazione del potere certificativo della Pubblica Amministrazione[55].

Inoltre la disciplina del referto digitale dovrà essere coordinata in modo opportuno e coerente con quella del Fascicolo Sanitario Elettronico di cui si è detto, con il quale, inevitabilmente, interagirà.

[55] Si veda in merito Cass. Pen. Sez. V n. 46172 del 29.11.2004. Si veda anche per il referto di Pronto Soccorso Tribunale civile di Cosenza, Sezione I, sentenza del 18 giugno 2007, n. 1048.

Per concludere, credo debba porsi attenzione al fatto che, in considerazione della particolare natura giuridica dei referti - non "semplici" documenti, né documenti "semplicemente" amministrativi, bensì documenti "speciali", in quanto espressione del potere certificativo del medico o di altro operatore sanitario in veste di pubblico ufficiale - essi non andranno considerati unicamente sotto profilo del loro contenuto (*dati* sanitari), ma anche con riferimento alla loro disciplina come insieme strutturato e logico di informazioni (*documento* sanitario).

7. La scheda sanitaria del medico di medicina generale

Uno dei compiti normativamente previsti del nostro medico di famiglia è quello della tenuta e dell'aggiornamento della nostra scheda sanitaria.

L'uso da parte del MMG della scheda sanitaria è stato previsto dal D.P.R. 28 luglio 2000, n. 270, il quale, all'art. 31, rubricato "Compiti del medico con compensi a quota fissa", prevede che tra i compiti del medico vi sia "la tenuta e l'aggiornamento di una scheda sanitaria individuale *ad uso del medico e ad utilità dell'assistito*, quale strumento tecnico-professionale che, oltre a migliorare la continuità assistenziale, consenta al medico di collaborare ad eventuali indagini epidemiologiche e a quanto previsto dagli accordi regionali".

Analoga previsione è contenuta nell'Accordo Collettivo Nazionale per la disciplina dei rapporti con i medici di medicina generale, sottoscritto ai sensi dell'art. 8 del d.lgs. 502/1992 del 2009[56], il cui art. 45, rubricato "Compiti del medico", precisa: "L'espletamento delle funzioni di cui al precedente comma 1 (cioè "funzioni e compiti individuali del medico di assistenza primaria") si realizza con:

(…) b) la tenuta e l'aggiornamento di una scheda sanitaria individuale, *su supporto informatico* (…) *ad uso del medico e ad utilità dell'assistito e del SSN, secondo standard nazionali e regionali e modalità definite nell'ambito degli Accordi regionali* (…)".

Da tale lettera b si desume la natura della scheda sanitaria quale documento di lavoro, la cui compilazione deve porsi quale primo obiettivo quello della salute dell'assistito e il cui impiego avverrà altresì ad utilità del Servizio Sanitario Nazionale.

[56] Accordo Collettivo Nazionale 23 marzo 2005, integrato con l'A.C.N. 29 luglio 2009.

La scheda è dunque uno strumento di lavoro del medico e deve servire alla tutela della salute del suo assistito.

Nel citato Accordo del 2009 è descritta come un documento "su supporto informatico" (quindi digitalizzata) e per questo motivo soggetta a standard nazionali e regionali. Tuttavia va posta attenzione al fatto che la visione della scheda sanitaria quale emerge dall'Accordo del 2009 è piuttosto diversa rispetto alle versioni precedenti.

In precedenza si trattava di un documento che veniva interpretato come ad esclusivo uso del medico e non se ne ipotizzava neppure una pubblicizzazione o una sottoposizione a standard.

Si trattava, quindi, di una sorta di diario medico cartaceo. Si legga infatti l'art. 19 dell'ACN del 1987: la tenuta e l'aggiornamento di una scheda sanitaria individuale vengono definiti *"ad esclusivo uso del medico, quale momento tecnico professionale"*[57].

Come si può notare, nell'Accordo del 1987 la scheda sanitaria veniva piuttosto vista come uno strumento di esclusivo utilizzo del medico e per sua propria necessità. Non venivano prescritte regole o formalità per la sua redazione.

Nell'accordo del 2009[58] invece, non solo si prevede che l'impiego sia "ad uso del medico" ma a "utilità dell'assistito": si prevede anche che essa debba essere in formato digitale e redatta secondo standard nazionali e regionali.

Progressivamente, quindi, la scheda sanitaria si è trasformata da "taccuino personale" del medico a documento formale e formalizzato di rilevanza esterna rispetto allo studio medico.

Tale processo si è svolto parallelamente a quello della organizzazione della medicina di gruppo che prevede soluzioni di informatizzazione e telematizzazione dello studio medico in modo da poter condividere agevolmente via rete i dati dei pazienti con i propri colleghi, qualora siano stati scelti come sostituti dall'assistito.

Il descritto processo evolutivo conduce dalla concezione della scheda sanitaria quale mero supporto alla memoria del professionista (e dunque destinato

[57] Decreto del Presidente della Repubblica 8 giugno 1987, n. 289, Accordo collettivo nazionale per la regolamentazione dei rapporti con i medici di medicina generale, ai sensi dell'art. 48 della legge 23 dicembre 1978, n. 833, pubblicato nella Gazz. Uff. 21 luglio 1987, n. 168, S.O. n. 1.

[58] Il più recente Accordo Collettivo Nazionale, quello dell'8 luglio 2010, non fa invece espressa menzione della scheda sanitaria individuale, ma vi si menziona il *"patient summary"*.

al suo esclusivo o prevalente impiego) alla sua considerazione come documento che va assumendo i caratteri della ufficialità e della finalità alla consultazione da parte di terzi, nonché della condivisione delle informazioni nell'ottica del bene del paziente e della continuità e coerenza delle cure.

La progressiva informatizzazione e ufficializzazione del scheda sanitaria comporta che essa debba essere considerata anche in ottica privacy, a tutela della riservatezza dei dati sanitari del paziente.

Una problematica che non si poneva (o non si poneva con questa gravità) quando la scheda sanitaria era documento riservato ad uso esclusivo del medico, medico tenuto al segreto professionale.

La necessità di una speciale cura e attenzione alla privacy in relazione alla scheda sanitaria sorge in particolare nel caso della medicina di gruppo, specie qualora i medici del gruppo realizzino tra loro una rete telematica e vi immettano le schede dei propri assistiti, affinché siano a disposizione del collega che li sostituisce[59].

In questo caso si pone il problema di configurare in modo corretto accessi e autorizzazioni al sistema informatico, in modo che esso consenta ai medici di vedere i dati sanitari dei pazienti dei colleghi solo se sono autorizzati a farlo, e cioè solo se ne sono sostituti autorizzati.

[59] Per un approfondimento sulle modalità e sulla regolamentazione dell'associazionismo medico si legga il mio articolo: C. Rabbito, La privacy nell'associazionismo medico, reperibile nella rivista telematica Telemeditalia, al link: http://www.telemeditalia.it/it/edizioni/edizioni/detail/0/177/1411/la-privacy-nellassociazionismo-medico-parte-second.html.

In sintesi, ai sensi del comma 6 dell'art. 54 dell'Accordo del 2009 le forma associative si distinguono in: medicina in associazione, medicina in rete, medicina di gruppo. Nel caso della **medicina in associazione** gli studi di assistenza primaria non sono vincolati ad una sede unica, ma sono distribuiti sul territorio. Non si fa cenno ad un eventuale collegamento di carattere informatico-telematico tra gli studi territorialmente distribuiti. Qualora mancasse ciò ne limiterebbe fortemente la funzione di continuità assistenziale non essendovi condivisione dei dati sanitari degli assistiti.

Nel caso, invece, della **medicina in rete**, non solo gli studi non vincolati ad una sede unica sono distribuiti nel territorio, ma si prevede il collegamento informatico-telematico tra essi, in modo tale che sia tecnicamente consentito l'accesso delle informazioni relative agli assistiti da parte di tutti i componenti dell'associazione (si sottolinea: *tecnicamente*, altro è la legittimità ai fini privacy). È, quindi, prevista la gestione da parte degli associati di schede sanitarie mediante software gestionali tra loro interoperabili.

La forma associativa della medicina in rete è, dunque, tra tutte quella che presenta una maggior vocazione tecnologica e che implica un sistema informatico-telematico più complesso e di più delicato inquadramento giuridico a fini privacy.

Nel caso della **medicina di gruppo**, a differenza che nella medicina in associazione e nella medicina in rete, la sede è unica e articolata in più studi medici. Si prevede un certo tasso di informatizzazione della sede, in quanto la scheda sanitaria deve essere informatizzata, gestita da software fra loro interoperabili e pertanto resa accessibile da parte dei medici, in quanto fruitori della rete locale installata nella sede.

Insomma: medicina di gruppo o in rete non significa che tutti i medici che sono in rete devono poter vedere (meno che mai effettuare modifiche) tutte le schede sanitarie dei pazienti dei colleghi.

Sotto il profilo giuridico, ciascuno medico di medicina generale è titolare del trattamento dei dati sanitari relativi ai suoi pazienti e, dunque, anche di quelli contenuti nella loro scheda.

Non è tuttavia conforme ai principi della privacy che tutti i medici possano accedere a tutti i dati di tutti i pazienti per il solo fatto di essere membri dell'associazione, né a maggior ragione è legittimo che tutti i medici siano abilitati alla modifica dei dati di tutti gli altri.

Un paziente, infatti, potrebbe accettare di essere curato, in sostituzione del proprio, solo da alcuni dei membri dell'associazione, in quanto non è obbligato ad accettare di essere curato da tutti i medici dell'associazione semplicemente in quanto membri dell'associazione. La scelta spetta al paziente, che potrebbe accettarne in sostituzione solo alcuni. E questo potrebbe verificarsi per un certo numero di pazienti di ciascuno degli associati.

Il medico sostituto, autorizzato a trattare – in sostituzione – i dati sanitari dei pazienti del collega, dovrà essere nominato responsabile dei dati dal collega, che ne è titolare e le la rete telematica dovrà essere strutturata con particolare attenzione in sede di configurazione degli accessi e delle autorizzazioni, al fine di rispettare la volontà dei pazienti che i loro dati siano visti e modificati solo dal medico scelto come sostituto.

Dovrebbero cioè essere configurati gli accessi in modo tale che solo se un medico è stato chiamato a fare la sostituzione e, quindi, è divenuto responsabile del trattamento dei dati sanitari di un determinato paziente possa vedere ed eventualmente modificare i dati del paziente "in condivisione".

Per concludere questa complessiva panoramica relativa alla documentazione sanitaria, credo sia importante sottolineare non solo la molteplicità dei documenti sanitari attualmente utilizzati, di cui molti sono in via di digitalizzazione, ma anche il fatto che essi siano caratterizzati da una loro storia e da una loro disciplina giuridica.

La loro collocazione e il loro ruolo all'interno del sistema sanitario (sempre di più anche "sistema informatico-telematico"), la loro storia e la loro natura

giuridiche vanno tenute bene in considerazione quando si procede alla loro informatizzazione.

Non solo, ma tutti gli aspetti sopra elencati sono fondamentali per capire quali problemi potrebbero nascere sotto il profilo della privacy e come risolverli. Oppure, dall'altro lato, per individuare i "falsi" problemi, che con la privacy non hanno nulla a che fare e che hanno già una semplice e lineare soluzione per mezzo di norme non recenti, ma ancora in vigore e che magari non sono direttamente attinenti alla privacy.

La realizzazione di un sistema di telemedicina che si voglia "calato" nel concreto, nella realtà della Sanità italiana attuale, non può prescindere dalla considerazione di tutto questo.

Un sistema di telemedicina è qualcosa di nuovo e di estremamente sperimentale che, mediante tecnologie recenti – ma non poi così nuove – si prefigge di interagire e di rapportarsi con un'organizzazione "vecchia", al fine di risolvere vecchi problemi con nuove soluzioni.

Per questi motivi non si può non tenere in considerazione l'esistente e come l'esistente sia stato finora disciplinato, con in aggiunta alcuni problemi "nuovi" o maggiormente acuiti a seguito dell'impiego delle nuove tecnologie, quale quello della privacy.

Si tratta indubbiamente di una sfida e di un'avventura, ma di una sfida non impossibile. Di una sfida che richiede solo la pazienza e la costanza di procurarsi e di utilizzare le "armi" corrette per affrontarla.

CAPITOLO QUARTO

BUONE PRATICHE PRIVACY PER UN PROGETTO DI TELEMEDICA

1. Il progetto di telemedicina e il diritto

Come si diceva la telemedicina e la sanità elettronica sono applicazioni piuttosto recenti, frutto delle nuove tecnologie informatiche e telematiche.

La novità non consiste ormai più nel "trovato" tecnologico, che non è poi così nuovo - anzi, in alcuni casi, esso ha parecchi decenni -, ma nel tentativo di un utilizzo sistematico e stabile di tali innovazioni all'interno dei sistemi sanitari nazionali, con l'obiettivo di far fronte in tempi rapidi e con continuità alle esigenze di cura dei pazienti, contenendo al tempo stesso le spese ed eliminando viaggi e passaggi burocratici inutili.

Ciò che è nuovo, quindi, non sono le applicazioni sperimentali della telemedicina e della sanità elettronica – quelle erano note da tempo - ma il tentativo di "calarle" in modo continuativo e sistematico, per i benefici che esse possono apportare, all'interno di un apparato burocratico quale il servizio sanitario di uno Stato, apparato che sappiamo essere complesso, articolato e regolamentato per certi aspetti da norme molto datate.

Innovare sotto il profilo scientifico e tecnologico, lo sappiamo, a volte è più agevole che innovare sotto il profilo amministrativo e più latamente giuridico.

Il diritto reagisce in maniera lenta alle innovazioni tecnologiche, e in modo indubbiamente lento il diritto italiano è risultato in grado di recepire tali innovazioni all'interno di un ordinamento che, non dobbiamo dimenticarlo, trova i suoi fondamenti nel diritto romano e che conserva ancora come vigenti alcune norme dei tempi in cui l'Italia era ancora una monarchia.

Tuttavia il processo di adeguamento, con accelerazioni e arresti improvvisi, è in corso, stimolato anche, certamente, dal contributo del legislatore europeo, il cui sguardo, concentrato sulla necessità di far funzionare sotto il profilo economico un organismo gigantesco come l'Unione, interpreta in modo molto positivo la diffusione del web e delle reti, sempre che il cittadino sia adeguatamente tutelato. Il legislatore europeo va avanti e non ammette stasi, va quindi seguito.

D'altro canto, sarebbe un errore aspettarsi una norma nuova e specifica per ognuna delle nuove creazioni tecnologiche, anche se destinate ad un campo delicato e importante come la Sanità.

In questi casi spesso si lamenta un vuoto legislativo e ci si sente orfani di un legislatore sollecito più spesso di quanto ciò non sia effettivamente necessario.

Si pensi, innanzitutto, che il processo di prevenzione, diagnosi, cura, assistenza coinvolge diritti fondamentali dell'individuo, quali la vita, l'integrità fisica, la salute, oltre al diritto che abbiamo ampiamente trattato, quello alla riservatezza.

Non possiamo quindi pensare che diritti così importanti non beneficino già di un'ampia e ben articolata tutela normativa e giurisprudenziale, e in caso di lacune (o apparenti lacune) normative è primariamente a questa tutela che dobbiamo fare riferimento.

Vi è poi una caratteristica fondamentale dell'ordinamento giuridico che va tenuta in considerazione: ciascun ordinamento giuridico, per la sua stessa sopravvivenza, si prefigge l'obiettivo della completezza e della coerenza interna.

Affinché cioè un ordinamento possa esistere nel tempo e sia in grado di regolamentare la vita di uno Stato esso deve presentare il minor numero possibile di situazioni non regolamentate e non ci devono essere contraddizioni interne tra le norme.

Per far fronte a questo alto livello di completezza, in caso di situazioni non espressamente previste si fa ricorso all'applicazione dei principi generali (cosiddetta *analogia juris*) e delle norme che disciplinano casi analoghi (cosiddetta *analogia legis*).

Nel caso italiano il ricorso all'analogia è disciplinato dall'art. 12 secondo comma delle disposizioni sulla legge in generale (o preleggi), poste in capo al Codice Civile, secondo cui in caso di mancanza di norme regolatrici "si ha riguardo alle disposizioni che regolano casi simili o materie analoghe e se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato".

Per comprensibili motivi, questa tecnica non può essere utilizzata in ambito penale e nel caso delle leggi eccezionali. Per il resto rimane affidato alla capacità dell'interprete e della corte giudicante fare ricorso a questa possibilità che il legislatore ci offre.

In molti casi quindi non ci serve una norma "nuova" e "à la page", ma basta cercare con cura ciò che fa al caso nostro e che è in vigore da tempo.

Dicevamo del lavoro dell'interprete: già perché per un compito di questo genere serve un giurista. Non possiamo pretendere che il tecnico, che ha già complicate questioni di progettazione e verifiche di funzionamento, o l'operatore sanitario, che deve sperimentare il sistema e lo deve tarare, si mettano anche alla ricerca delle norme giuridiche, che inquadrino correttamente il nuovo apparato nel mondo del diritto.

La telemedicina e la sanità elettronica richiedono una mente aperta, un approccio necessariamente interdisciplinare e la stretta collaborazione tra professionalità diverse, non ultimo il giurista, se possibile un giurista non digiuno dai fondamenti delle ICT[60] e della medicina.

Il giurista ha un compito importante: supportare i tecnici e gli operatori del mondo sanitario nella difficile opera di comprensione e di completamento del quadro normativo di riferimento.

Egli non deve avere un atteggiamento di censura o di ammonimento, non deve semplicemente snocciolare le norme in modo apatico e distaccato, deve spiegarne la *ratio* agli altri professionisti e insieme si deve cercare il modo di conformarsi il meglio possibile a quanto il legislatore richiede.

In quest'opera il giurista non potrà prescindere dal costante consapevole riferimento alla Carta costituzionale e dalla considerazione delle diverse fonti del diritto (leggi, decreti, regolamenti, linee guida, pareri di Autorità), avendo ben chiaro il loro differente "peso" in ragione della loro posizione nella gerarchia delle fonti.

Per poter capire bene i problemi e per poterne studiare insieme le soluzioni è però necessario che l'operatore del diritto sia messo a conoscenza dei dettagli del sistema telemedico, non nel senso di una conoscenza dei mezzi tecnologici impiegati comparabile a quella di un esperto del settore, ma nel senso di una adeguata comprensione sistemi implementati e delle prestazioni fornite che gli consenta di individuare le criticità giuridiche e di consigliare di conseguenza.

[60] Information Communications Technologies.

Ma la sua funzione non potrà limitarsi ad una identificazione degli aspetti "sensibili" e vulnerabili in relazione all'applicazione del quadro giuridico in vigore, il che già richiede da parte sua intuito, sensibilità e una conoscenza non superficiale del settore, ma dovrà arrivare fino alla proposta di soluzioni concrete, le quali, calando le norme astratte nella effettiva realizzazione del sistema informatico-sanitario, ne rendano possibile l'attuazione.

L'operatore del diritto, infatti, è consapevole del fatto che non tutto ciò che è tecnicamente possibile è anche giuridicamente lecito e sa che dovrà cercare insieme all'ingegnere, all'informatico, al medico e all'imprenditore che investe, soluzioni che siamo lecite e tecnologicamente ed economicamente accettabili.

La sua funzione avrà, prima di tutto e soprattutto un carattere "logico", nel senso strettamente etimologico del termine[61].

2. Il *Businness Process Reengineering*

Ciò che si chiede oggi ad un progetto di telemedicina è che esso sia in grado di superare la soglia della sperimentalità e di diventare a tutti gli effetti un prodotto, un sistema adottabile in modo stabile e duraturo in un servizio socio-sanitario nazionale reale e con concrete caratteristiche, regole e limiti.

Una applicazione telemedica sarà quindi tanto più apprezzabile e spendibile quanto più è in grado di inserirsi nell'esistente e di "colloquiare" con i sistemi presenti.

Per questo motivo molto spesso - e specie con riguardo a quelle applicazioni che si prefiggono anche o prevalentemente l'informatizzazione della parte amministrativa dell'attività sanitaria -, è opportuno conoscere approfonditamente i processi che si intendono informatizzare e telematizzare.

Le applicazioni ICT non devono, infatti, ricostruire non in cartaceo una mera copia dell'esistente, piuttosto, per sfruttare al meglio le loro potenzialità, è con-

[61] Il termine deriva dalla parola greca "*logos*", ragione. L'idea del *logos* in Grecia risale ad Eraclito (540-480 a.C.). Per essa si intende: "arte del ben ragionare", nonché "quella parte della filosofia che insegna a dirigere la ragione verso la verità". Il *logos* è il principio universale attraverso il quale tutte le cose sono collegate e tutti gli eventi naturali accadono.

sigliabile prima "ripensare" il processo cui si intendono applicare e migliorarlo, fin dove possibile, grazie a quelle stesse potenzialità.

A questo fine può essere utile una tecnica detta di *business process reengineering*, le cui basi sono state gettate negli anni Novanta e che è stata poi successivamente aggiornata [62]. Ritengo che essa sia particolarmente efficace nella informatizzazione di eventi sanitari che hanno anche o prevalentemente una componente amministrativa.

Il cosiddetto BPR prevede uno studio del processo che si intende innovare che si articola in tre fasi: una prima in cui si definisce il campo di applicazione dell'intervento; una seconda di rilevazione dei processi e di diagnosi delle modalità con cui vengono realizzate le attività, tenendo conto dello stato attuale (cd. *as-is*); una terza di riprogettazione.

La fase di esame dello stato attuale è indispensabile al fine di individuare le eventuali aree di miglioramento; infine si deve procedere alla (ri)progettazione destinata alla definizione dei processi sulla base delle problematiche emerse nelle fasi di diagnosi (cd. *to be*).

Lo scopo dell'analisi è, quindi, quello prendere in considerazione e di individuare le esigenze di cambiamento e di informatizzazione, ripensando e razionalizzando i processi organizzativi contestualmente all'ideazione dei sistemi informatici a supporto dei processi stessi. Si dovrà pertanto procedere ad applicare l'informatica solo laddove essa sia realmente necessaria e si interverrà sull'organizzazione qualora invece le lacune siano di tipo organizzativo e l'applicazione forzosa dell'informatica non potrebbe apportare particolari benefici.

Il principale obiettivo del BPR è quello di comprendere nei dettagli come un'attività venga effettivamente realizzata in un dato momento, chi la fa, quali siano le relazioni interne tra gli agenti, qual sia l'organizzazione che supporta tale attività.

Un altro aspetto molto importante e molto utile, anche sotto il profilo delle applicazione delle norme sulla privacy, è quello relativo allo studio del flusso informativo: come è strutturato il flusso delle informazioni? Quali informazioni "viaggiano", verso quali destinazioni e a quale scopo?

[62] M. Hammer, *The reengineering Revolution,* Harper Collins, New York, 1995.

Vi è poi un aspetto dello studio del flusso informativo che interessa moltissimo il giurista e che va contemplato sicuramente nel nostro BPR: lo studio della documentazione.

Quali tipi di documenti vengono utilizzati? Quale ne è la semantica più comune? Nell'ambito del documento in quale posizione si trovano le informazioni rilevanti? Ma soprattutto: qual è il valore giuridico di quel determinato documento (es. atto pubblico, documento amministrativo, documento con mera rilevanza interna etc…)? Come la norma richiede che esso sia redatto, firmato, inviato, consegnato?

Dunque, l'analisi dei processi deve necessariamente articolarsi in una molteplicità di dimensioni, quali:

- analisi dell'organizzazione, intesa come l'insieme delle risorse che erogano e amministrano il servizio;
- analisi funzionale, e quindi dei flussi informativi, che circolano all'interno dell'attuale sistema;
- analisi degli aspetti normativi che vincolano e regolano l'attuale operatività.

Qualora, per esempio, il sistema oggetto di studio si prefigga l'erogazione di un servizio a favore del cittadino da parte del nostro Servizio Sanitario Nazionale (si pensi all'invio del referto in formato digitale, alla comunicazione telematica all'INPS dei certificati di malattia, al Fascicolo Sanitario Elettronico), la reingegnerizzazione comporterà opportunamente non solo la riorganizzazione delle sequenze di azioni e se necessario del flusso documentale, ma avrà ricadute sulla stessa ristrutturazione dei procedimenti amministrativi sottesi ai processi che si informatizzano, al fine di correggere eventuali difformità rispetto alla regolamentazione normativa e di evitare al tempo stesso ridondanze e duplicazioni nei passaggi interni.

L'informatica e la telematica che aiutano ad applicare la norma al meglio, con meno perdite di tempo e più velocemente: questo sarebbe il più ambizioso obiettivo perseguibile.

Naturalmente nel settore pubblico (o comunque in ambiti fortemente regolamentati) potrebbe non essere possibile procedere ad un ripensamento di servizi, attività e strutture così ampio e profondo come è invece possibile talora nel settore privato (ovvero in settori poco regolamentati).

La peculiare missione rivolta al bene pubblico e l'attività distintiva di un'organizzazione dello Stato comportano la necessità di conformarsi ad una dettagliata disciplina normativa. Ne discende che ogni ipotesi di reingegnerizzazione e successivamente di informatizzazione e telematizzazione di un settore fortemente regolamentato (quale in Italia quello della Sanità) deve assumere necessariamente la normativa vigente come uno dei vincoli di progettazione dei nuovi sistemi.

D'altro canto – sotto opposta prospettiva - le ipotesi di reingegnerizzazione e le iniziative di automazione possono suggerire utili proposte di modifica normativa, che trovano nelle iniziative di semplificazione legislativa un naturale canale di attuazione.

La realizzazione di un sistema di sanità elettronica rende a mio giudizio fortemente consigliabile una preventiva analisi con il metodo BPR, in considerazione della molteplicità e diversità delle variabili coinvolte: la specificità dei servizi forniti, la centralità del cittadino-paziente contrapposta alla molteplicità dei soggetti pubblici e privati coinvolti nell'erogazione, la necessaria partecipazione della pubblica amministrazione e degli organismi sanitari, l'intervento dell'imprenditoria privata, la diversità delle piattaforme tecnologiche di partenza.

Come si potrà facilmente capire in situazioni come queste il supporto dell'operatore del diritto risulta indispensabile: tra le differenti possibili ipotesi di riorganizzazione che i tecnici sono in grado di suggerire, solo il giurista, infatti, potrà individuare quella o quelle che, senza sacrificare la componente tecnologica, siano anche rispettose del quadro normativo, specie in considerazione del fatto che quest'ultimo è in continua evoluzione, è potenzialmente incompleto o può richiedere l'applicazione di norme analogiche o di principi generali dell'ordinamento.

Risulta assolutamente indispensabile nella fase progettuale di un sistema telemedico e nelle seguenti fasi realizzative una stretta collaborazione tra i professionisti del diritto, i tecnici e i funzionari amministrativi.

3. La privacy: quando entra in scena?

Il rispetto delle norme italiane ed europee sulla privacy nella fase di progettazione e realizzazione di un sistema di telemedicina non è questione da poco.

Si tratta di un aspetto che non va assolutamente sottovalutato, ma che va tenuto in considerazione fin dall'inizio: fin dalla fase di ideazione del progetto.

Progettare un sistema di telemedicina, sotto tutti i profili (medici, tecnologici, deontologici, economici), realizzarlo nella sua componente *hardware*, in quella *software*, verificarne i risultati sotto il profilo medico, testarlo e - quando si è giunti ad un livello di funzionamento che si ritiene adeguato -, porsi il problema se esso sia "anche" a "norma privacy" è un grave errore. Un errore da evitare assolutamente.

Considerato che il diritto alla privacy è costituzionalmente tutelato, sarebbe come mettere in piedi un'attività d'impresa complessa, costosa, potenzialmente molto remunerativa, ma che poi si scopre non possa essere attuata in quanto viola un diritto costituzionalmente tutelato in più Stati. Un buco nell'acqua.

La carenza in questo caso è di tipo logico e riguarda il modo di rapportarsi ad un sistema di *e-health*: lo si pensa solo come una fantastica applicazione di tecnologia, un'eccezionale espressione della scienza.

Ci si concentra nell'opera di realizzare questo straordinario prodotto della competenza umana e poi ci si ferma a contemplarlo. Ma si sa che ci sono – in ogni Stato – balzelli e lacciuoli burocratici. Uno di questi viene considerato essere la privacy. Allora, in un secondo tempo, si interviene con qualche "limatina", affinché anche la privacy sia "a posto".

Procedere così è un rischio. Un rischio prima di tutto economico, in quanto si potrebbe dover ricominciare da capo. Una perdita di tempo, e quindi di denaro.

La privacy e, più in generale, gli aspetti giuridici di un sistema di telemedicina non vanno considerati un *frame*, una cornice esterna, come a volte purtroppo si sente dire.

Se la si pensa come una cornice, come qualcosa di "esterno" che contorna e "colloca" un oggetto in un determinato spazio - quello spazio che il legislatore ci ha concesso - non si capisce il vero ruolo della privacy.

Essa va pensata come una delle regole fondanti, come lo sono, nel caso della telemedicina, le regole della fisica, della medicina o dell'informatica.

Così come, quando si concepisce un sistema di telemedicina, lo si pensa tenendo conto delle imprescindibili leggi della fisica, delle regole della informatica, delle conoscenze della medicina, allo stesso modo lo si deve pensare, poi organizzare, infine realizzare "insieme" alle regole della privacy.

Il sistema deve essere "pensato" e deve crescere con le regole della privacy: essa ne deve essere uno degli ingredienti essenziali, non una decorazione finale.

La anticipazione in fase progettuale della considerazione della privacy e delle sue declinazioni è del resto pienamente conforme con quanto ci raccomanda il legislatore europeo. Come abbiamo visto il regolamento europeo privacy introduce il nuovo concetto di *privacy by design*, che comporta che chi realizza un prodotto o un software debba necessariamente progettarlo contestualmente alle misure di sicurezza che gli dovranno essere applicate, e quindi con piena conoscenza degli eventuali pericoli e delle situazioni di rischio, che devono essere preventivamente "tamponate" o meglio "evitate".

Quanto detto fin qui significa, in pratica, anche un coinvolgimento, fin dall'inizio dei lavori, di figure professionali (i giuristi, gli esperti di misure di sicurezza, i medici legali) che fino ad ora venivano consultate solo alla fine - a sistema avviato – o addirittura solo al sorgere di qualche difficoltà.

4. Le buone pratiche privacy in un progetto di telemedicina

Ma veniamo all'atto pratico: volendo realizzare un sistema di telemedicina rispettoso della privacy oggi in Italia, quali sono gli aspetti di cui principalmente tener conto?

Innanzitutto non va dimenticato che l'attuale quadro normativo in materia, già di per sé articolato e in evoluzione, sarà significativamente innovato dall'entrata in vigore del regolamento comunitario di cui si è detto[63].

Nella progettazione di un sistema di telemedicina che operi (anche) in Italia non si potrà, quindi, non preoccuparsi di verificare cosa prescriva il regolamento, poiché ben presto esso sarà vincolante anche nel nostro Paese e, per di più, lo sarà senza norme "di intermediazione" - come è successo finora con le direttive -, ma mediante la diretta applicazione all'interno del nostro ordinamento dei suoi articoli. Le nostre norme interne che si pongano in contrasto con esso dovranno essere disapplicate.

[63] Si veda il paragrafo terzo del primo capitolo.

Una bella rivoluzione. E una rivoluzione complicata se si pensa a quante questioni interpretative, discussioni, dibattiti, interpretazioni dottrinarie e giurisprudenziali si origineranno dalla necessità di individuare le norme incompatibili che andranno disapplicate.

I temi del regolamento che potrebbero maggiormente incidere nella realizzazione di un sistema di telemedicina sono sicuramente quello della menzionata *privacy by design* e quello del cosiddetto *privacy impact assessment*[64].

Inoltre va considerata la rilevanza che il legislatore europeo pone alla raccolta del consenso dell'interessato, che deve essere sempre esplicito, mai supposto e il rilievo riconosciuto al diritto all'oblio, cioè il diritto dell'interessato (e quindi del paziente) ad essere "dimenticato", ad essere cioè cancellato dal web o dalla banca dati quando il trattamento non sia più giustificato.

Un altro passo fondamentale per la correttezza di un sistema di telemedicina sotto il profilo della privacy è l'analisi del profilo soggettivo, cioè l'individuazione dei "protagonisti"[65]: dato per appurato che l'interessato i cui dati vengono trattati è necessariamente il paziente, si tratta di verificare chi sono il titolare o i contitolari e chi i responsabili, ricordando che in ambito sanitario molto spesso sia titolari che responsabili sono persone giuridiche, non persone fisiche.

L'individuazione giuridica del titolare è fondamentale sotto il profilo della disciplina da applicare. Si deve ricordare infatti che il dato personale a contenuto sanitario è dato sanitario *solo* se è trattato da titolari che sono organismi sanitari o esercenti professioni sanitarie, e inoltre che per essere tale deve essere utilizzato a tutela della salute dell'interessato, di terzi o della collettività.

Se il titolare non è un organismo sanitario o non è un esercente una professione sanitaria, ma, per esempio, è un'impresa o un'associazione, siamo in presenza sì di un dato personale arricchito da una informazione a contenuto sanitario, ma *a rigori* non di un "dato sanitario".

Si deve quindi porre attenzione al fatto che l'insieme delle norme del Codice che si devono applicare cambia a seconda delle natura giuridica del titolare e a seconda della finalità del trattamento (e spesso le due cose fanno di pari passo).

[64] Si veda in merito pagina 11.

[65] Si veda il secondo paragrafo del capitolo secondo.

Se i requisiti del titolare (organismo sanitario o esercente professione sanitaria) e della finalità (tutela della salute) ci sono tutti, allora ci si deve rifare alla specifica regolamentazione contenuta nel Titolo V, altrimenti siamo in presenza di un dato sensibile e quindi si deve applicare la relativa disciplina contenuta anch'essa nel Codice[66].

Vi sono tuttavia delle situazioni particolari, rispetto a quanto detto, che sono menzionate nella Autorizzazione del Garante al trattamento dei dati idonei a rivelare lo stato di salute[67]. In questa Autorizzazione, il Garante preso atto del fatto che un elevato numero di trattamenti idonei a rivelare lo stato di salute è effettuato per finalità di prevenzione o di cura, per la gestione di servizi socio-sanitari, per ricerche scientifiche o per la fornitura all'interessato di prestazioni, beni o servizi e che i relativi dati sensibili (tali sono i dati idonei a rivelare lo stato di salute se trattati non da organismi sanitari o da esercenti professioni sanitarie) possono essere trattati dai soggetti privati e dagli enti pubblici economici solo previa sua autorizzazione e, ove necessario, con il consenso scritto degli interessati, autorizza appunto tale trattamento. E lo autorizza nei seguenti casi:

a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana anche con riguardo a studi nell'ambito della sperimentazione clinica di farmaci, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. *In tali casi occorre acquisire il consenso*, e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati.

[66] Per la quale si riporta alle pagine 34 e segg.

[67] Autorizzazione n. 2/2011 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 24 giugno 2011, pubblicata sulla Gazzetta Ufficiale n. 162 del 14 luglio 2011.

b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;
c) alle persone fisiche e giuridiche, alle imprese, anche sociali, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi.

Supponiamo quindi che i dati idonei a rivelare lo stato di salute siano trattati, in un contesto di telemedicina, non da un organismo sanitario o da un operatore sanitario, ma da un'associazione o altro organismo privato (o da una persona fisica) per finalità di ricerca, oppure da un'organizzazione di volontariato per gli scopi che si è prefissata in base allo statuto, oppure da un'impresa, per fornire all'interessato beni, prestazioni o servizi, tutti questi soggetti non dovranno, pur trattando dati indubbiamente sensibili, preoccuparsi di ottenere l'autorizzazione del Garante, in quando hanno già la "copertura" di questa Autorizzazione generale.

D'altro canto, occorre fare attenzione: il Garante in questa autorizzazione ci dice espressamente che la finalità di ricerca scientifica o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, non esimono chi tratta i dati necessari all'attività di ricerca dalla necessità di conformarsi agli adempimenti previsti dal Codice.

Il Garante in questa occasione ci ricorda che la "sperimentalità" di un progetto in cui si trattano dati idonei a rivelare lo stato di salute delle persone non esime chi li tratta dalla necessità di preoccuparsi della tutela della privacy e dei conseguenti obblighi previsti dal nostro ordinamento. In due parole: la sperimentalità non scusa l'approssimazione o la negligenza.

Questo vale anche per le soluzioni tecnologiche telemediche che, per molta parte della loro vita, specie in Italia, rimangono purtroppo nel limbo della sperimentalità e della progettualità, senza approdare, a volte mai, a sistema e/o a prodotto.

In questi casi, nonostante l'impiego della telemedicina possa essere ricondotto ad una dimensione sperimentale, temporanea, precaria o non sia stato consacrato da un idoneo atto amministrativo, i dati trattati sono dati veri di

pazienti veri: risulta quindi indispensabile un adeguamento agli obblighi, anche di carattere più burocratico, richiesti dalle norme privacy.

5. La squadra in campo: responsabili e incaricati

Al fine di una gestione degli aspetti privacy efficace e stabile, il titolare deve conoscere la "squadra" che lo aiuterà in quest'opera delicata e affidare ai suoi membri i compiti necessari, con adeguate istruzioni.

Il titolare, quindi – che come si diceva poc'anzi in ambito sanitario è molto spesso una persona giuridica – deve procedere alla nomina dei suoi "luogotenenti", cioè delle persone, siano esse fisiche o giuridiche che concretamente si occuperanno della gestione dei dati in base alle sue indicazioni[68].

È opportuno che il titolare scelga consapevolmente e accuratamente i suoi responsabili, in quanto essi rappresenteranno la sua *longa manus* nella gestione dei dati. Ciò vale tanto più nel caso cui il titolare (ad esempio un'ASL o un'azienda ospedaliera) intendano affidare in esterno, in *out-sourcing*, la gestione di una serie di servizi informatico-telematici, ad esempio l'invio dei referti telematici, la archiviazione e conservazione della documentazione sanitaria digitalizzata, la gestione del sito internet, ivi comprese le aree riservate che consentono il "colloquio diretto" con i pazienti, lo *storage* dei dati del sistema, la stessa manutenzione e l'aggiornamento dei *server* aziendali.

In questo caso, chi si occupa di questi servizi dovrà essere nominato responsabile esterno e gli dovranno essere date istruzioni molto rigorose e precise, a massima tutela dei dati sanitari dei pazienti.

A loro volta i responsabili (siano essi persone fisiche o enti) dovranno provvedere alla nomina degli incaricati[69], cioè di coloro che materialmente opereranno sui dati. Anche quella dell'incaricato è figura da non trascurare in quanto, in ambito sanitario, l'incaricato tratta dati di estrema delicatezza e deve essere adeguatamente preparato per farlo.

[68] È possibile trovare due modelli di nomina di responsabili nell'Appendice di questa trattazione, uno relativo alla nomina di responsabile interno e uno alla nomina di responsabile esterno.

[69] Un modello di nomina è reperibile nell'appendice.

A questo scopo è sicuramente d'uopo nella lettera d'incarico inserire clausole di avvertimento e sensibilizzazione per l'incaricato, il quale molto spesso è un operatore sanitario e quindi è già vincolato dal segreto che gli impone la sua professione, ma potrebbe anche non esserlo: si potrebbe trattare di un funzionario amministrativo, di un operatore del data center o del call center[70], di un tecnico che si occupa della manutenzione e dell'aggiornamento del sistema.

Nel caso di incaricati al trattamento che non siamo vincolati al segreto per ragioni di deontologia professionale, il legislatore ha previsto di estendere a questi i medesimi vincoli del personale sanitario che essi supportano e coadiuvano[71].

Anche il responsabile esterno, specie se tratta dati idonei a rivelare informazioni sanitarie, dovrà provvedere alla nomina dei suoi incaricati, nella quale dovrà chiarire al suo personale la rilevanza dei dati trattati e impegnarlo a gestire i dati con particolare cura e nel rispetto delle misure di sicurezza stabilite.

Mentre nel caso dei responsabili interni ed esterni si presume che il rapporto titolare – responsabile sia piuttosto duraturo, nel caso degli incaricati può succedere che l'attività di trattamento dei dati da parte dell'incaricato sia di breve durata. Questo può verificarsi per i più vari motivi: potrebbe trattarsi di un rapporto di lavoro a sua volta breve (es. una prestazione occasionale), di un rapporto afferente all'apprendimento (es. stage, borsa di studio), di una collaborazione per motivi di ricerca scientifica[72].

In questi casi il legislatore ritiene che sia sufficiente, in luogo della lettera di incarico, la firma da parte dello stagista, del ricercatore, del borsista, del professionista che effettua una prestazione occasionale, di una semplice lettera di impegno alla riservatezza, il cui contenuto, tuttavia, non si discosterà di molto da quello dell'incarico formale, salvo per la temporaneità del vincolo di collaborazione.

[70] Si pensi, ad esempio, agli operatori dei Centri Unificati di Prenotazioni (CUP) dell'ASL che esistono in molte città italiane.

[71] Articolo 83 comma 2 lettera i.

[72] Come si può facilmente immaginare in un progetto di telemedicina e/o di sanità elettronica questo tipo di situazioni sono molto frequenti.

La strutturazione della équipe da parte del titolare - anche sotto il profilo formale mediante le lettere di nomina e di incarico -, è un adempimento molto importante che questi deve porre in essere, in modo da sapere con un discreto grado di certezza qual è la sua "squadra" e seguendo quali regole – che in molta parte lo stesso titolare stabilisce – tale squadra giocherà la difficile partita della tutela dei dati personali dei pazienti.

Naturalmente la preparazione della squadra non si otterrà semplicemente con l'atto formale della presentazione della lettera di nomina o di incarico, per quanto il loro contenuto sia completo e aggiornato: il momento formativo del personale è fondamentale e deve essere effettuato il prima possibile, con l'ulteriore previsione di occasioni di aggiornamento periodico.

La formazione dovrà riguardare sia i fondamenti e i concetti-chiave della privacy, quanto la spiegazione delle misure di sicurezza da applicare, non solo nel senso di un mero elenco di quelle da adottare ma anche mediante un approfondimento di tipo tecnico sulla loro natura: una formazione quindi il meno possibile didascalica ma piuttosto operativa e ragionata.

Un aspetto fondamentale di una efficace organizzazione del personale in ottica privacy nel caso di impiego delle tecnologie informatiche e telematiche consisterà nella assegnazione delle modalità di autenticazione degli utenti al sistema informatico e, ancora più importante, della profilazione delle autorizzazioni. Il titolare, oppure il responsabile delegato, dovranno stabilire per ciascun utente e tenendo conto del ruolo, della funzione, dell'attività che tale utente è chiamato a svolgere all'interno del sistema, se egli può accedere e soprattutto, una volta che sia entrato, quale tipo di attività è autorizzato a svolgere: che dati può semplicemente vedere? Quali dati può integrare o addirittura correggere? Può scaricare dei dati e memorizzarli altrove?

La profilazione delle autorizzazioni, specie in un sistema di informatica sanitaria, è importantissima, perché il personale che potrebbe avere necessità di accedere è numeroso, con le più svariate funzioni (si va da chi si occupa dell'acquisto dei farmaci per l'ospedale al primario di un reparto) e i dati contenuti sono quasi interamente informazioni sulla salute dei pazienti[73].

[73] A proposito della profilazione delle autorizzazioni si veda quanto già detto in merito alla medicina di gruppo a pagina 65 e seguenti.

Le scelte che sottendono alla profilazione delle autorizzazioni devono essere fatte dal titolare o dal responsabile in modo competente (essi devono conoscere le caratteristiche delle attività che vengono svolte attraverso il sistema informatico) e coscienzioso, con la consapevolezza della natura delicata dei dati trattati.

Nel caso di un progetto di telemedicina sarà opportuno procedere fin dall'inizio alla strutturazione di questa "squadra" che opera sui dati, al fine di sensibilizzare i protagonisti e di vincolarli fin dall'avvio alla correttezza nel trattamento del dato: la sperimentalità del progetto non deve essere considerata una ragionevole motivazione per essere approssimativi o frettolosi con riguardo al trattamento dei dati dei pazienti.

Anzi, proprio per il fatto che si sta creando qualcosa di nuovo, ma dalla configurazione ancora variabile, che tuttavia già "maneggia" dati di grandissima rilevanza, tutte le varie e diversificate professionalità che sono coinvolte nella realizzazione della innovazione creativa (chi progetta l'hardware, chi il software, chi immette i dati, chi li valuta, coloro stessi che ne esporranno i risultati in sede convegnistica) devono essere consapevoli che ciò che si sta facendo è – per quanto progettuale e precario - estremamente reale per il paziente, i cui dati veri ed effettivi si stanno trattando.

Lo stesso dicasi circa la necessità di procedere in modo responsabile e preparato anche in un progetto telemedico alla profilazione delle autorizzazioni all'interno del sistema informatico, (autorizzazioni poi possono anche essere variate a mano a mano che il progetto procede, ma è meglio cominciare fin da subito a realizzarle): il personale che accede ai dati è vario, ha compiti diversi e molti non di natura strettamente sanitaria: meglio sforzarsi di stabilire fin dall'inizio chi può vedere i dati, quali dati può vedere e per compiere quali operazioni.

Naturalmente quanto detto per un *progetto* di telemedicina, in termini di necessità di strutturazione anche formale, di profilazione delle autorizzazioni e di preparazione consapevole del personale operante, varrà tanto più per un *prodotto* di telemedicina o di sanità elettronica che sia operante con continuità e stabilmente all'interno o tra organismi sanitari.

6. Il beneficiario della "macchina – privacy": il paziente

Un aspetto che va sempre tenuto presente con riguardo a tutto l'impianto di carattere burocratico e tecnico della tutela dei dati e che può aiutare a comprendere e "metabolizzare" tutte le energie che la tutela della privacy, specie in ambito sanitario, richiede è il fatto che l'obiettivo è la salvaguardia del paziente.

Il paziente è il nostro fine e il nostro metro, è al paziente che dobbiamo ricordare i suoi diritti mediante l'informativa, è il paziente che dobbiamo, grazie all'informativa, rendere edotto del fatto che l'attività di cura prevede l'apporto di tecnologie telematiche (quindi suscettibili di arrecare una serie di benefici ma anche seri pericolo) e di cui, a seguito del rilascio dell'informativa, dobbiamo raccogliere il consenso.

Nel caso in cui a trattare il dato a contenuto sanitario sia un titolare/organismo sanitario o, in proprio, un esercente la professione sanitaria, si tratterà di dati sanitari, i quali quindi ricadono nella disciplina di cui all'articolo 76 e seguenti del Codice: sarà sufficiente il consenso dell'interessato.

Qualora invece il titolare non sia un organismo sanitario o un professionista sanitario i dati idonei a rivelare lo stato di salute saranno da considerarsi dati sensibili e quindi andrà applicato l'articolo 20 del Codice nel caso di trattamento da parte di soggetti pubblici e dagli articoli 23 e 26 congiuntamente nel caso del trattamento da parte di privati.

L'articolo 20 prevede che il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Il legislatore però aggiunge che nei casi in cui una disposizione di legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati dall'ente con suo regolamento. Se nessuna di queste condizioni è verificata, è necessaria un'autorizzazione apposita del Garante.

Quindi per il trattamento di dati sensibili (quindi anche dei dati a contenuto sanitario) da parte di un soggetto pubblico è necessario: 1) una disposizione di legge, oppure 2) la legge + il regolamento, oppure 3) l'autorizzazione del Garante. Non si richiede invece il consenso dell'interessato.

Nel caso invece in cui a trattare dati a contenuto sanitario sia un privato (es. un'impresa) si applica l'articolo 23 che prevede che: "Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato". In particolare, ai sensi dell'art. 26 "i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante". Risulterebbe quindi necessario il consenso + un'autorizzazione apposita del Garante.

Tuttavia, come si è detto al paragrafo quarto di questo capitolo, il Garante provvede periodicamente a rilasciare un'autorizzazione di carattere generale relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, nella quale autorizza il trattamento da parte di soggetti privati, senza escludere l'obbligo, naturalmente, della raccolta del consenso dell'interessato.

Nei casi in cui sia necessario raccogliere il consenso, la predisposizione di un'informativa quanto più possibile chiara e circostanziata risulta essenziale, con specifica indicazione – se del caso - del fatto che vengono impiegate tecnologie informatico-telematiche ed eventualmente che l'interessato sta partecipando ad un progetto di telemedicina, di teleassistenza e/o di sanità elettronica.

Non sempre il consenso dovrà o potrà essere firmato dall'interessato[74].

Qualora il dato debba essere necessariamente trattato per salvare la vita o l'incolumità fisica dell'interessato e l'interessato stesso non possa dare il proprio consenso in quanto si trovi fisicamente impossibilitato, sia stato interdetto o si trovi in uno stato di incapacità di intendere e di volere, il consenso può essere dato, al suo posto, ex art. 24 comma primo lettera e del Codice, da chi esercita la potestà genitoriale (se minore) o dal tutore (in caso di incapacità d'agire), oppure da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato[75].

È molto importante tenere conto di questa particolarità nel caso di un progetto di telemedicina, in quanto potrebbe capitare, come nel caso del progetto Telecoma, di trattare dati di pazienti in situazioni di incapacità - sia pure differentemente graduate - e dunque risulterà necessaria la raccolta del consenso presso i soggetti che possono esprimere la volontà al trattamento dei dati in

[74] Si veda anche quanto già accennato al paragrafo 6 del capitolo secondo.

[75] Si veda un esempio di questo tipo di consenso nell'allegato 6.

luogo del paziente, appunto: esercenti la potestà, prossimi congiunti, familiari, conviventi.

A completamento di quanto previsto dall'articolo 24, l'articolo 82 prevede il caso in cui il paziente si trovi in stato di impossibilità fisica, di incapacità di agire o incapacità di intendere o di volere dell'interessato e non sia possibile acquisire il consenso da chi esercita legalmente la potestà, o da un prossimo congiunto, da un familiare, da un convivente e neppure dal responsabile della struttura presso cui dimora l'interessato.

In questo caso, la presentazione dell'informativa e la raccolta del consenso *possono essere posticipati a dopo la prestazione sanitaria*.

La posticipazione degli aspetti – diciamo così – più "burocratici" di rilascio dell'informativa e di raccolta del consenso è anche assolutamente giustificata in due casi che il legislatore prende – correttamente – in considerazione:

1) l'eventualità in cui la situazione sia molto grave: c'è il rischio di un danno imminente e irreparabile alla salute o all'incolumità fisica dell'interessato. La gravità del rischio fa propendere il legislatore nel senso di posticipare la raccolta del consenso affinché sia effettuato prima l'intervento sanitario, che in questo caso ha importanza primaria[76];
2) il caso in cui il fattore tempo sia essenziale: l'intervento sanitario deve essere fatto subito, altrimenti perde di efficacia. La situazione non è così grave evidentemente come nel caso precedente, ma bisogna fare in fretta. Anche qui le problematiche relative alla privacy cedono il passo ad altri diritti di livello costituzionale: la salute, l'integrità fisica. Effettuato quanto necessario dal punto di vista sanitario, si procederà a rendere l'informativa e a raccogliere il consenso[77].

Come si diceva, in luogo dell'interessato sono abilitati a rilasciare il consenso, in casi particolari, le seguenti persone: chi esercita legalmente la potestà, un prossimo congiunto, un familiare, un convivente o, in loro assenza, il responsabile della struttura presso cui dimora l'interessato.

[76] Articolo 82 comma 2 lettera b.

[77] Articolo 82 comma 3.

Un'altra figura di rilievo, la cui individuazione risulta utile agli operatori sanitari e assistenziali, è il cosiddetto *"caregiver"* detto anche, a volte, "familiare di riferimento".

L'identificazione e la segnalazione nel fascicolo del paziente/assistito del cosiddetto "familiare di riferimento" è sicuramente molto utile a chi si occupa, vuoi sotto il profilo sanitario, vuoi sotto il profilo assistenziale, del malato, dell'anziano, di chi sia bisognoso di assistenza.

Alcuni *software* di telemedicina o di teleassistenza consentono all'utente l'indicazione, a beneficio del medico, dell'infermiere, dell'assistente sociale o dell'operatore socio-sanitario, del familiare di riferimento.

Tuttavia è bene tenere sempre presente che il *caregiver* o il "familiare di riferimento" non sono figure inquadrate normativamente, non hanno deleghe, autorizzazioni o poteri specifici solo per il fatto di essere stati individuati come tali dagli operatori.

Si tratterà di vedere di volta in volta, in base al tipo di legame che collega il *caregiver* (che potrebbe anche non essere un familiare[78]) al paziente, a seconda dello stato di salute e psichico del paziente e a seconda della scelta o dell'atto giuridico da compiere, se il *caregiver* sia abilitato a fare quella scelta o a compiere quell'atto in luogo del paziente.

Nel caso specifico del consenso privacy, potrebbe capitare che il *caregiver* e/o il familiare di riferimento rientrino tra coloro che sono abilitati dal Codice a firmare il consenso al trattamento dei dati ma *potrebbero anche non essere compresi nell'elenco del legislatore*.

Inoltre va precisato che secondo un'accreditata interpretazione della norma, la sequenza dei soggetti che si possono sostituire all'interessato per la firma del consenso va intesa nell'ordine di importanza in cui il legislatore l'ha posta: prima gli esercenti la potestà, poi i congiunti, poi i familiari, poi i conviventi e solo, in loro assenza, il responsabile della struttura presso cui dimora l'interessato.

[78] In situazioni particolari, in assenza di altri familiari, ho potuto riscontrare l'assegnazione della funzione di *caregiver* alla badante. In questi casi l'operatore deve tenere conto del fatto che le badanti spesso provengono da altri paesi e che quindi ci potranno essere delle difficoltà di tipo linguistico e di comprensione degli istituti del diritto italiano.

Prendendo quindi in considerazione l'ipotesi in cui ci sia un *caregiver*, va prima appurato se tale *caregiver* rientri nell'elenco fatto dal legislatore e poi se non vi sia qualcuno disponibile alla firma che il legislatore non abbia considerato più "importante": se, per esemplificare, il *caregiver* identificato sia una badante convivente, ma nell'occasione specifica sia presente un figlio, va data la precedenza al figlio.

Con riguardo alla comunicazione dei dati sanitari, come sappiamo, ai sensi dell'articolo 84, le comunicazioni che riguardano il suo stato di salute possono essere date all'interessato solo tramite il medico che sia stato scelto dall'interessato o, in subordine, dal titolare (ad esempio l'azienda ospedaliera). Qualora l'interessato non sia in grado di riceverle, possono essere date ai soggetti di cui all'art. 82 che abbiamo più volte menzionato.

Va, quindi, tenuto in considerazione il fatto che, per una corretta applicazione della norma, i soggetti in gioco che si "sostituiscono" al paziente incapace in differenti e diversamente rilevanti occasioni potrebbero essere tre: il *caregiver*, il familiare che ha espresso il consenso al trattamento dei dati sanitari dell'assistito e il familiare che ha ricevuto le informazioni sullo stato di salute dell'assistito.

In ambito telemedico, quando si procede alla configurazione del fascicolo dell'assistito, va tenuto conto di questi tre differenti ruoli e, al fine di supportare in ogni caso possibile l'operatore sanitario, vanno indicate e distinte le persone di riferimento per ciascuno di questi tre aspetti.

Come si è già detto[79], il Codice della privacy, a tutela della riservatezza dei dati sanitari prevede anche particolari misure di sicurezza a tutela della dignità del paziente: in particolare l'art. 83 ribadisce l'obbligo per i titolari dei trattamenti in ambito sanitario di adottare anche soluzioni di tipo organizzativo, nella strutturazione delle prestazioni e dei servizi che coadiuvino la tutela della privacy e il rispetto del segreto professionale.

Ci chiede, infatti, il legislatore di prestare attenzione ad adottare tutte quelle soluzioni che siano utili alla massima tutela della dignità dell'interessato, soprattutto in quelle particolari situazioni in cui il suo contatto con la struttura sanitaria

[79] Capitolo secondo paragrafo 8.

avviene contestualmente alle altre persone, al fine di evitare una accidentale conoscenza da parte di terzi delle informazioni sanitarie che lo riguardano.

Come è facile intuire, nel caso della telemedicina e della teleassistenza le situazioni di promiscuità tra pazienti o che potrebbero in ogni caso mettere a repentaglio la debita tutela della riservatezza del paziente sono minori, specie nel caso in cui le soluzioni tecnologiche siano finalizzate a portare soccorso e assistenza al paziente fino al suo domicilio. Ma non è comunque escluso che si possano verificare, sia in quanto le prestazioni telemediche potrebbero non essere erogate al domicilio, ma per esempio in un centro sanitario di servizio, per quanto vicino al domicilio del paziente, sia in quanto a casa del paziente possono comunque crearsi delle situazioni di promiscuità, sia pure di tipo diverso (es. i parenti non direttamente coinvolti ma in visita, i vicini di casa, etc…).

Nel caso poi in cui alla telemedicina si faccia ricorso in quelle situazioni di soccorso particolari per cui essa è nata (soccorso in mare, zone isolate perché montagnose o insulari), l'idea che la particolarità del frangente e l'urgenza dell'intervento facciano un po' "abbassare" la guardia sulla tutela della privacy non è affatto peregrina.

Bisogna invece sforzarsi di preoccuparsene sempre: per esempio anche in mezzo all'oceano, solo quella parte dell'equipaggio che è deputato a farlo dovrà conoscere i dati del paziente, non l'intera nave.

7. Il percorso delle informazioni e i documenti in cui sono contenute

La tutela dei dati nei sistemi di telemedicina e di sanità elettronica si realizza attraverso un altro aspetto fondamentale: quello della gestione delle informazioni.

È importantissimo, al fine della realizzazione di un sistema informatico-telematico rispettoso della riservatezza del paziente e dei suoi familiari, che fin dalla fase progettuale si analizzi il tipo di informazioni che il sistema tratta, quale ne sia il percorso all'interno del sistema e come tali informazioni vengano poi archiviate e conservate. Solo in questo modo sarà possibile comprendere quali regole devono essere osservate e quali misure di sicurezza vadano applicate.

L'informazione va studiata dal suo formarsi e fino alla sua destinazione finale, per poter comprendere quali pericoli si annidino durante per percorso per la privacy dell'interessato.

Collegato a questo aspetto si deve tenere anche conto di un altro essenziale profilo: molto spesso in ambito sanitario non si ha a che fare con una informazione singola o con molte informazioni dello stesso tipo, ma con informazioni che sono organizzate secondo un ordine logico ormai stabilito dalla tradizione e dalla prassi, oltre che dal diritto: i documenti.

Molti di tali documenti, come si è ampiamente mostrato, sono portatori di una loro propria disciplina giuridica, formata da norme, da decisioni della giurisprudenza, da elaborazioni dottrinarie. È assolutamente necessario che si tenga conto della disciplina giuridica di ciascun documento sanitario.

Trascurare la natura giuridica di un documento, sia pure digitalizzato, significherebbe vanificare lo sforzo di conformità alla privacy, finendo per rendere il sistema illegittimo per altri versi (oltre che spesso anche sotto l'aspetto privacy).

Sarà quindi opportuna un'approfondita conoscenza della natura giuridica dei documenti sanitari che si intendono digitalizzare e delle responsabilità civili, penali e amministrative connesse al regime giuridico particolare di ciascun documento impiegato.

Qualora poi, come spesso accade, si proceda alla realizzazione di una banca dati contenente informazioni di tipo sanitario, sarà opportuno conformarsi alle indicazioni del Codice relative alla creazione di un data base sanitario, distinguendo e scindendo i dati a contenuto nominativo dalle informazioni sanitarie, come illustrato nel paragrafo 11 del secondo capitolo.

Data la delicatezza di dati trattati, in nessun caso si dovranno trascurare le misure minime di sicurezza prescritte e, con riguardo alle misure preventive, data la novità e la sperimentalità dei sistemi tele medici, il livello di cura nella loro predisposizione dovrà essere mantenuto alto, più di quanto non avvenga normalmente nei sistemi sanitari.

In un sistema di telemedicina concretamente utilizzato all'interno del nostro SSN, i soggetti coinvolti che alimentano con le loro informazioni e con documenti la banca dati potrebbero essere molti (ospedale, medico di famiglia, servizi sociali). La "cartella clinica digitale" (in senso non tecnico in questo caso) di ciascun paziente potrebbe essere ampia e formata da molti elementi informativi.

Vale la pena in questi casi non trascurare le indicazioni del Garante a proposito del FSE, in quanto per certi versi ciò che si creerebbe è una sorta di piccolo fascicolo sanitario del paziente. In particolare dovranno essere tenuti in considerazione due principi che il Garante afferma: il principio di autodeterminazione e il diritto all'oblio.

Ne discende che anche nel caso della telemedicina e della sanità elettronica, il paziente dovrà sempre essere tenuto informato circa l'esistenza di una sorta di *cartella clinica digitale* che lo riguarda e il suo mantenimento e aggiornamento non dovranno mai essere effettuati all'insaputa o contro la volontà del paziente.

Nel caso della cessazione del sistema, a tutela del paziente i suoi dati dovranno essere cancellati, non potranno essere utilizzati per fini che non siano attinenti alla sua salute e qualora si volessero conservare per il loro particolare valore scientifico, dovranno essere anonimizzati.

8. L'abolizione del DPS: che fare?

Il Decreto Legge n. 5 del 9.2.2012[80] recante "Disposizioni urgenti in materia di semplificazione e di sviluppo", poi convertito con la legge di conversione del 4 aprile 2012, n. 35, all'art. 45 "Semplificazioni in materia di dati personali" prevede l'abolizione del Documento Programmatico di Sicurezza.

In particolare, tale articolo recita: "Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni: (omissis...) all'articolo 34 è soppressa la lettera g) del comma 1 ed è abrogato il comma 1-bis; d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26".

È stata quindi soppressa la lettera g) del comma 1 ed è stato abrogato il comma 1-bis dell'art. 34 del Codice privacy, cioè *non vi è più obbligo di "tenuta di un aggiornato documento programmatico sulla sicurezza"* (art. 34, comma 1, lett. g).

Per quanto riguarda invece il disciplinare tecnico, sono soppressi i paragrafi da 19 a 19.8, cioè è revocato *l'obbligo di presentare "entro il 31 marzo di ogni*

[80] Pubblicato nel supplemento ordinario alla G.U. n. 33 del 9 febbraio 2012.

anno", da parte del "titolare di un trattamento di dati sensibili o di dati giudiziari", *"un documento programmatico sulla sicurezza"*.

Come si ricorderà, la redazione del Documento Programmatico di sicurezza era obbligatoria in base a quanto previsto nel Codice privacy e nel collegato disciplinare tecnico: entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari doveva redigere anche attraverso il responsabile, tale documento contenente importanti informazioni con particolare riguardo a:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombevano sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Il DPS doveva inoltre contenere, in base a quanto stabilito al punto 19.7., la descrizione dei criteri per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare.

Per i dati personali idonei a rivelare lo stato di salute e la vita sessuale il punto 19.8 richiedeva l'individuazione dei "criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato"[81].

Ai fini della compilazione del DPS, il Garante privacy aveva messo a punto una "Guida operativa per redigere il documento programmatico di sicurezza" disponibile al link: www.garanteprivacy.it/garante/document?ID=1007740.

[81] Per questo aspetto si rimanda a quanto detto nel paragrafo 11 del secondo capitolo.

Nella premessa alla Guida, il Garante precisava che essa si prefiggeva di facilitare l'adempimento dell'obbligo di redazione del DPS nelle organizzazioni di piccole e medie dimensioni o, comunque, non dotate al proprio interno di competenze specifiche. Essa pertanto poteva essere d'ausilio nella predisposizione del DPS, ma non era obbligatorio utilizzarla.

Uno degli aspetti più complessi e discussi in relazione alla redazione di un corretto e completo DPS era quello relativo all'analisi dei rischi che incombono sui dati (19.3): si richiedeva infatti la descrizione dei principali eventi potenzialmente dannosi per la sicurezza dei dati e ne dovevano essere valutate le possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati.

La redazione del DPS veniva sentita spesso come un adempimento puramente formale, che nulla aggiungeva alla consapevolezza (o meno) circa la necessità di proteggere i dati con adeguate misure di sicurezza, né incrementava la sensibilità del personale sulle problematiche della riservatezza, specie dei dati sensibili e sanitari.

Insomma, era da molti considerato un orpello inutile e dispendioso in termini di tempo e di denaro. Il legislatore ha quindi ritenuto opportuno abolire questo obbligo, in quanto, e su questo possiamo condividere pienamente la *ratio* del provvedimento, quello che è veramente importante non né che delle misure di sicurezza venga redatta una chiara e brillante rassegna scritta, quanto che le misure di sicurezza vengano consapevolmente, coscienziosamente, adeguatamente adottate.

Per quanto non sia più obbligatoria la tenuta di un aggiornato DPS, chi scrive non può che caldeggiare, per una efficace tutela dei dati, che venga tenuta traccia, in modo organico e coordinato in un apposito documento delle misure di sicurezza effettivamente adottate.

La creazione e la tenuta di un tale dossier faciliterà la raccolta delle informazioni in caso di eventuali verifiche da parte delle autorità preposte e ridurrà pertanto la probabilità di incorrere in sanzioni.

Ne discende che anche se la tenuta di un aggiornato DPS non è più un obbligo, mi sento di consigliare vivamente specie nel caso di applicazioni di telemedicina e di sanità elettronica, la redazione di un documento – periodica-

mente aggiornato - contenente una sorta di resoconto del tipo di dati trattati e delle misure di sicurezza adottate.

Il DPS, così come normativamente previsto e la sua Guida operativa, potranno poi costituire una sorta di modello dello strumento analitico e di sintesi ad uso del titolare e del privacy manager per poter applicare e gestire al meglio le misure di sicurezza e, quindi, per mantenere la qualità, la correttezza, la disponibilità e l'obbligatoria riservatezza del dato clinico.

Allegato 1
LA NOMINA DEL RESPONSABILE

Atto di nomina di responsabile del trattamento ex art. 29 del d.lgs. 196/2003 ai fini della realizzazione di……
(indicare l'attività che richiede il trattamento dei dati)

(Nome del titolare ente o persona fisica), nella Sua qualità di titolare del trattamento ai sensi dell'art. 28 del d.lgs.196/2003,

PREMESSO CHE

il d.lgs.196/2003 (cd Codice della Privacy) ha espressamente previsto la possibilità che il titolare preponga al trattamento dei dati personali uno o più responsabili, scelti tra soggetti che, per la loro capacità, esperienza e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela dei dati personali, ivi compresa la sicurezza degli stessi;
che il responsabile deve procedere al trattamento con la dovuta diligenza, nonché attenendosi alle istruzioni ricevute dal titolare, il quale deve vigilare sulla puntuale osservanza delle disposizioni vigenti;

(NOME DEL TITOLARE)

intende procedere alla nomina di ……. (inserire qui gli estremi del RESPONSABILE) responsabile del trattamento, per ciò che attiene ai dati personali (sensibili, sanitari) di cui è titolare in relazione al (descrizione dell'attività del titolare) e il cui trattamento è necessario per lo svolgimento della suddetta attività.
Il titolare dichiara che i dati affidati al responsabile sono:

1. esatti e aggiornati;
2. pertinenti, completi e non eccedenti la finalità della raccolta;
3. raccolti e trasmessi al responsabile in modo lecito.

Il titolare autorizza il responsabile ad affidare, sotto la responsabilità di quest'ultimo, l'esecuzione di operazioni di trattamento a incaricati che per esperienza,

capacità ed affidabilità, forniscano anche idonea garanzia del pieno rispetto della legge, con particolare riguardo alla sicurezza.
Il responsabile nominerà quali incaricati le persone fisiche cui è affidato il servizio.
Ove necessario, il titolare potrà nominare soggetti terzi quali ulteriori responsabili o incaricati del trattamento dei suoi dati.
Il responsabile impartirà le necessarie istruzioni e disposizioni vincolanti ai propri incaricati.

TANTO PREMESSO, NOMINA RESPONSABILE DEL TRATTAMENTO
……, affidandogli i compiti e le responsabilità previste dall'art. … del D.Lgs.196/2003.

Con la sottoscrizione del presente atto, **(INSERIRE IL NOME DEL RESPONSABILE)** accetta la nomina e s'impegna a procedere al trattamento dei dati di cui (NOME ENTE O PERSONA FISICA) è titolare, attenendosi alle istruzioni impartite.

A questi fini, il titolare impartisce al responsabile le seguenti istruzioni:
1. Il responsabile deve:
a) operare nel rispetto dei principi generali fissati dall'art. 11 del d.lgs.196/2003;
b) impartire ai propri incaricati le istruzioni fornite dal titolare del trattamento, nonché imporre le precauzioni generali dettate dal d .lgs.196/2003;
c) adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare,
d) vigilare sul rispetto delle misure di sicurezza da parte dei soggetti incaricati,
e) tenere la lista degli incaricati con l'indicazione dell'ambito di trattamento consentito mediante strumenti elettronici e quella del trattamento mediante strumenti non elettronici,
f) effettuare esclusivamente i trattamenti indicati dal titolare.
2. I dati trasmessi dal titolare al responsabile *(descrizione dati e natura degli stessi)* sono stati raccolti e trattati nel pieno rispetto della legge; in particolare, sono state già fornite le informative e raccolti i consensi previsti dalla legge. Il responsabile provvederà a tali adempimenti solo previe esplicite istruzioni impartite per iscritto dal titolare.
3. Il titolare ha, altresì, provveduto ad adempiere ogni obbligo di legge relativo alla sicurezza dei dati personali, ai sensi del d.lgs.196/2003.
   Dal canto suo, il Responsabile provvederà a tutelare la sicurezza dei dati nella propria sfera di operatività.

4. Il responsabile deve adoperarsi per garantire l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 D.Lgs.196/2003, nell'ambito della propria sfera di operatività.
5. Il responsabile dichiara di impegnarsi a relazionare a richiesta del titolare sulle misure di sicurezza adottate .

La nomina a responsabile cesserà (indicare il termine dell'attività), salvo espresso rinnovo.

……(Luogo), lì .....(data)

IL TITOLARE (firma)_____

Il responsabile espressamente dichiara di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali (eventualmente: sensibili e sanitari) e, come tali, sono soggetti all'applicazione del Codice per la protezione dei dati personali e si obbliga ad ottemperare agli obblighi previsti dal suddetto Codice.

IL RESPONSABILE _____

Allegato 2
LA NOMINA DEL RESPONSABILE ESTERNO

Atto di nomina di responsabile esterno del trattamento ex art. 29 del d.lgs. 196/2003 ai fini della realizzazione di……
(indicare l'attività che richiede il trattamento dei dati)

(NOME DEL TITOLARE, ENTE O PERSONA FISICA), nella Sua qualità di titolare del trattamento ai sensi dell'art. 28 del d.lgs.196/2003,

PREMESSO CHE

il d.lgs.196/2003 (cd Codice della Privacy) ha espressamente previsto la possibilità che il titolare preponga al trattamento dei dati personali uno o più responsabili esterni, scelti tra soggetti che, per la loro capacità, esperienza e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela dei dati personali, ivi compresa la sicurezza degli stessi;

CHE il responsabile esterno deve procedere al trattamento con la dovuta diligenza, nonché attenendosi alle istruzioni ricevute dal titolare, il quale deve vigilare sulla puntuale osservanza delle disposizioni vigenti;

(NOME TITOLARE)

intende procedere alla nomina di …….(inserire qui gli estremi del RESPONSABILE ESTERNO) in qualità di responsabile del trattamento, per ciò che attiene ai dati personali (sensibili e sanitari) di cui è titolare in relazione a (indicare l'attività nell'ambito della quale si intendono trattare i dati) e il cui trattamento è necessario per lo svolgimento della suddetta attività.

Il titolare dichiara che i dati trasmessi al responsabile esterno sono:

1. esatti e aggiornati;
2. pertinenti, completi e non eccedenti la finalità della raccolta;
3. raccolti e trasmessi al responsabile in modo lecito.

Il titolare autorizza il responsabile esterno ad affidare, sotto la responsabilità di quest'ultimo, l'esecuzione di operazioni di trattamento a incaricati che per esperienza, capacità ed affidabilità, forniscano anche idonea garanzia del pieno rispetto della legge, con particolare riguardo alla sicurezza.
Il responsabile nominerà quali incaricati le persone fisiche cui è affidato il servizio.
Ove necessario, il titolare potrà nominare soggetti terzi quali ulteriori responsabili o incaricati del trattamento dei suoi dati.

Il responsabile impartirà le necessarie istruzioni e disposizioni vincolanti ai propri incaricati.

TANTO PREMESSO, NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO

(NOME DEL RESPONSABILE, ENTE O PERSONA FISICA), affidandogli i compiti e le responsabilità previste dall'art. 29 del D.Lgs.196/2003.

Con la sottoscrizione del presente atto, **(INSERIRE IL NOME DEL RESPONSABILE)** accetta la nomina e s'impegna a procedere al trattamento dei dati di cui (NOME DEL TITOLARE) è titolare, attenendosi alle istruzioni impartite.
A questi fini, il titolare impartisce al responsabile le seguenti istruzioni:

1. Il responsabile deve:

a) operare nel rispetto dei principi generali fissati dall'art. 11 del d.lgs.196/2003;
b) impartire ai propri incaricati le istruzioni fornite dal titolare del trattamento, nonché imporre le precauzioni generali dettate dal d.lgs.196/2003;
c) adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare,
d) vigilare sul rispetto delle misure di sicurezza da parte dei soggetti incaricati,
e) tenere la lista degli incaricati con l'indicazione dell'ambito di trattamento consentito mediante strumenti elettronici e quella del trattamento mediante strumenti non elettronici,
f) effettuare esclusivamente i trattamenti indicati dal titolare.

2. I dati trasmessi dal titolare al responsabile **(inserire la descrizione dati e natura degli stessi)** sono stati raccolti e trattati nel pieno rispetto della legge; in particolare, sono state già fornite le informative e raccolti i consensi previsti dalla legge. Il responsabile provvederà a tali adempimenti solo previe esplicite istruzioni impartite per iscritto dal titolare.
3. Il titolare ha, altresì, provveduto ad adempiere ogni obbligo di legge relativo alla sicurezza dei dati personali, ai sensi del d.lgs.196/2003.
   Dal canto suo, il Responsabile provvederà a tutelare la sicurezza dei dati nella propria sfera di operatività.
4. Il responsabile deve adoperarsi per garantire l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 D.Lgs.196/2003, nell'ambito della propria sfera di operatività.

5). Il responsabile dichiara di impegnarsi a relazionare a richiesta del titolare sulle misure di sicurezza adottate .

La nomina a responsabile cesserà (indicare scadenza della nomina), salvo espresso rinnovo.

……(Luogo), lì……(data)

IL TITOLARE (firma)_____

Il responsabile espressamente dichiara di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali (eventualmente: sensibili, sanitari) e, come tali, sono soggetti all'applicazione del Codice per la protezione dei dati personali e si obbliga ad ottemperare agli obblighi previsti dal suddetto Codice.

IL RESPONSABILE _____

Allegato 3
LA NOMINA DI INCARICATO

Atto di nomina di incaricato del trattamento di dati personali e sensibili al fine……
(indicare sinteticamente l'attività per cui è necessario il trattamento del dato)

(NOME DEL TITOLARE, ENTE O PERSONA FISICA), nella Sua qualità di titolare (oppure NOME DEL RESPONSABILE, nella Sua qualità di responsabile) del trattamento dei dati in relazione alla realizzazione della seguente attività (sintetica descrizione dell'attività per cui è necessario il trattamento del dato), ai sensi dell'art. 30 del d. lgs. n. 196/2003,

designa quale incaricato al trattamento dei dati personali e sensibili
il Sig./la Sig.ra (nome e cognome), nato/a a……,
il ……..., in servizio presso ……..
(**inserire indicazione di: ufficio/area/funzione**).

Tale nomina riguarda il trattamento di dati personali e sensibili ai quali il soggetto sopracitato abbia accesso in relazione alla realizzazione di … (descrizione dell'attività che richiede il trattamenti dei dati) nell'espletamento della funzione che gli è propria, nelle mansioni e/o per gli incarichi che gli/le sono stati affidati.
Il Sig./la Sig.ra …… potrà quindi trattare i dati necessari allo svolgimento delle sue mansioni.
In particolare, in ottemperanza al d.lgs. 196/2003, ai sensi del quale costituisce *trattamento* "qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati", e in relazione al presente atto di nomina, il Sig./la Sig.ra …… dovrà trattare i dati personali e sensibili attenendosi alle seguenti modalità:

1) in modo lecito e secondo correttezza;
2) raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta;
3) verificando, ove possibile, che siano esatti e, se necessario, aggiornarli;
4) verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile/titolare;

Più generalmente, il trattamento dovrà essere realizzato in osservanza delle norme di cui al d.lgs. 196/2003 e delle prescrizioni che verranno impartite dal titolare/responsabile del trattamento.
In quanto incaricato del trattamento, il Sig./la Sig.ra ..... avrà accesso alle seguenti banche dati e/o archivi:

.....

Il Sig./la Sig.ra ..... si impegna a rispettare altresì le misure attinenti alla sicurezza che gli/le verranno impartite dal titolare/responsabile.
In particolare, in relazione ai trattamenti effettuati con strumenti elettronici, ai sensi dell'Allegato B del d.lgs. 196/2003, si ricorda che il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo (oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave) [inserire la modalità di identificazione prescelta dal titolare].

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
Gli incaricati dovranno adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
La parola chiave è composta da almeno otto caratteri (oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito); essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave e' modificata almeno ogni tre mesi.
Le credenziali sono disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
Sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incari-

cato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
Inoltre, potrà essere utilizzato un sistema di autorizzazione che comporterà l'individuazione di profili di ambito diverso per i differenti incaricati.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, verranno individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

[Il titolare può, in questa sede, specificare le modalità di autenticazione dell'incaricato e le sue autorizzazioni (chi è – quali dati può vedere – cosa può fare in relazione a tali dati: consultazione, correzione, modifica, integrazione, memorizzazione – quali dati può inserire/modificare/cancellare) o demandare tali informazioni a piani operativi o regolamenti interni. Nonché indicare le modalità per la sostituzione in caso di assenza o impedimento dell'incaricato e le istruzioni di custodia degli strumenti. Si consiglia di provvedere in questa stessa sede ad illustrare tutti questi aspetti per semplicità].

Luogo e data……

Firma del titolare/responsabile del trattamento dei dati o dei rispettivi rappresentati legali se si tratta di enti

Allegato 4
LA NOMINA DI INCARICATO MEDIANTE LETTERA DI RISERVATEZZA

Lettera di riservatezza ai fini del trattamento di dati personali e sensibili in relazione alla mansione/funzione/incarico di ……

Il/La Sig./Sig.ra …… (inserire nome e cognome), nato/a ……, il ……, in servizio presso …… (inserire ufficio/area/funzione), nel periodo (inserire date di permanenza all'interno dell'ente o dell'incarico) …… , nella Sua qualità di …… (inserire mansione/funzione/incarico),

SI IMPEGNA

con la presente lettera di riservatezza al trattamento dei dati personali, sensibili e sanitari di cui verrà a conoscenza per causa e nello svolgimento delle sue mansioni, come sopra indicate, con modalità conformi al d. lgs. n. 196/2003 (Codice della Privacy) e in ogni caso in modo lecito e secondo correttezza.
In particolare, in ottemperanza al d.lgs. 196/2003, ai sensi del quale costituisce trattamento "qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati", e in relazione al presente atto, il Sig./la Sig.ra ……
si impegna a trattare i dati personali, sensibili e sanitari attenendosi alle seguenti modalità:

1) in modo lecito e secondo correttezza;
2) raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta;
3) verificando, ove possibile, che siano esatti e, se necessario, aggiornarli;
4) verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile/titolare;
5) altro (……).

Più generalmente, il trattamento dovrà essere realizzato in osservanza delle norme di cui al d.lgs. 196/2003 e delle prescrizioni che verranno impartite dal titolare/responsabile del trattamento.

Il Sig./la Sig.ra …… avrà accesso alle seguenti banche dati e/o archivi: ……
Il Sig./la Sig.ra …… si impegna a rispettare altresì le misure attinenti alla sicurezza che gli/le verranno impartite dal titolare/responsabile del trattamento.

In particolare, in relazione ai trattamenti effettuati con strumenti elettronici, ai sensi dell'Allegato B del d.lgs. 196/2003, si ricorda che il trattamento di dati personali con strumenti elettronici è consentito solo a coloro che sono dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata conosciuta solamente dal medesimo (oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave).

A questi fini il Sig./la Sig.ra ……si impegna ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

[Il titolare può, in questa sede, specificare le modalità di autenticazione dell'incaricato e la sua sfera di autorizzazione (chi è – quali dati può vedere – cosa può fare in relazione a tali dati: consultazione, correzione, modifica, integrazione, memorizzazione – quali dati può inserire/modificare/cancellare) o demandare tali informazioni a piani operativi o regolamenti interni. Nonché indicare le modalità per la sostituzione in caso di assenza o impedimento dell'incaricato, le istruzioni per l'accesso del sostituto e per la custodia degli strumenti. Si consiglia di provvedere in questa stessa sede ad illustrare tutti questi aspetti per semplicità].

Luogo e data ……

Firma ……

Allegato 5
INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

(D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali")

CONSENSO DELL'ASSISTITO AL TRATTAMENTO DEI SUOI DATI

Gentile Assistito/Assistita,
la presente comunicazione ha lo scopo di informarLa che il decreto legislativo 196/2003 (cd. Codice della Privacy) prevede la tutela dei dati personali, nel pieno rispetto dei diritti e delle libertà fondamentali, oltre che delle norme sul segreto professionale.
Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.
I Suoi dati personali, i Suoi dati sensibili e i Suoi dati sanitari, ove Lei acconsenta firmando l'apposito modulo che Le verrà consegnato dagli operatori di …… (indicare riferimenti del titolare o del responsabile), verranno raccolti per …… (indicare l'attività per cui è necessario il trattamento dei dati), come più dettagliatamente spiegato in …… (indicare eventuali allegati che illustrino l'attività), che Le è stata consegnato insieme alla presente informativa.

Ai fini del Codice della Privacy, La si informa di quanto segue:

1. Finalità del trattamento
   I Suoi dati personali, con particolare riferimento a quelli riferiti al Suo stato di salute, saranno trattati per … (indicare l'attività per cui è necessario il trattamento dei dati).
   Si tratta di …… (illustrare, volendo, l'attività con maggior dettaglio).

2. Modalità del trattamento
   a) Titolare del trattamento è (nome e cognome, indirizzo e recapito del titolare se persona fisica, riferimenti, indirizzo della sede e recapiti del titolare se ente).
   b) Il trattamento dei dati è effettuato direttamente dal titolare, tramite il personale sanitario e amministrativo, nonché tramite personale consulente o convenzionato.
   c) Il trattamento è eseguito sia con strumenti manuali che informatico-telematici, comunque con l'osservanza di misure di sicurezza in grado di garantire che solo personale autorizzato possa conoscere le informazio-

ni che riguardano la persona assistita e i suoi familiari e di ridurre al minimo i rischi di perdita, distruzione o accesso non autorizzato ai suoi dati.

d) In relazione al trattamento eseguito con strumenti informatico-telematici si specifica che tale trattamento potrà essere effettuato con modalità di telemedicina e teleassistenza.
e) Il trattamento dei Suoi dati è necessario per poter effettuare le prestazioni richieste e/o necessarie per la tutela della Sua salute. Il Suo mancato consenso al trattamento dei dati, con l'eccezione dei trattamenti urgenti ai sensi dell'articolo 82 del Codice e di quelli disposti da Autorità Pubblica, potrà comportare l'impossibilità dello svolgimento dell'attività di cura.
f) Il Responsabile del trattamento è (nome e cognome del responsabile se persona fisica, riferimenti del responsabile se ente).

3. Ambito di comunicazione dei dati
   l Suoi dati anagrafici, anamnestici e clinici saranno resi disponibili al personale sanitario, tecnico e amministrativo afferente a (indicare ente, amministrazione, organismo, struttura, dipartimento, area etc che si occuperà del trattamento dei dati) - nei limiti delle competenze di ciascun operatore - per le attività di diagnosi, cura, prevenzione e riabilitazione, nonché per le attività di carattere amministrativo, di controllo di gestione e di rendicontazione.

4. Diritti dell'interessato
   Sono riprodotte di seguito le norme dell'art. 7 della citata legge, che stabiliscono i diritti dell'interessato in relazione al trattamento dei dati personali:
   1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
   2. L'interessato ha diritto di ottenere l'indicazione:
      a) dell'origine dei dati personali;
      b) delle finalità e modalità del trattamento;
      c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
      d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 del Codice della Privacy;
      e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

CONFERIMENTO DEL CONSENSO

Si precisa che:
il trattamento sarà avviato con il consenso scritto dell'interessato e previa lettura della presente informativa.

Il sottoscritto/a _____
nato/a a _____ il _____
e residente in _____

dichiara di aver preso visione delle informazioni riportate nel documento "INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI" allegato ed esprime altresì il proprio consenso al trattamento e alla comunicazione dei propri dati personali e sanitari.

Firma di presa visione ed accettazione.

_____

Data _____ Luogo_____

Allegato 6
INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

(D. Lgs. 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali")

CONSENSO DEL FAMILIARE AL TRATTAMENTO DEI DATI DELL'ASSISTITO[82]

Gentile Familiare,
la presente comunicazione ha lo scopo di informarLa che il decreto legislativo 196/2003 (cd. Codice della Privacy) prevede la tutela dei dati personali, nel pieno rispetto dei diritti e delle libertà fondamentali, oltre che delle norme sul segreto professionale.
Secondo la normativa indicata, tale trattamento dovrà essere improntato ai principi di correttezza, liceità, trasparenza e di tutela della riservatezza e dei diritti della persona assistita.
I dati personali, i dati sensibili e i dati sanitari della persona assistita, ove Lei acconsenta firmando l'apposito modulo che Le verrà consegnato dagli operatori di … (indicare riferimenti del titolare o del responsabile), verranno raccolti per la realizzazione di … (indicare l'attività per cui è necessario il trattamento dei dati), come più dettagliatamente spiegato in … (indicare eventuali allegati che illustrino l'attività), che Le è stata consegnato insieme alla presente informativa.
Viene richiesto il Suo consenso al trattamento dei dati personali, sensibili e sanitari della persona assistita in quanto ai sensi del Codice della Privacy (art. 82, comma 2, lett. a) il consenso è validamente manifestato, in luogo di chi si trova in situazioni di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere, da chi esercita la potestà genitoriale, la tutela o l'amministrazione di sostegno ovvero da un familiare, da un prossimo congiunto, dal convivente.
Ai fini del Codice della Privacy, La si informa di quanto segue:

1. Finalità del trattamento
   I dati personali dell'assistito, con particolare riferimento a quelli attinenti allo stato di salute, saranno trattati per … (indicare l'attività per cui è necessario il trattamento dei dati).
   Si tratta di …… (illustrare, volendo, l'attività con maggior dettaglio).
   Per "trattamento del dato", ai sensi dell'art. 4 comma 1 del Codice della Privacy, si deve intendere: qualunque operazione o insieme di operazioni, ef-

[82] Questo modulo può essere firmato da genitori, tutori, familiari, prossimi congiunti o dal convivente al posto della persona assistita, se questa si trova in stato di impossibilità fisica, incapacità di agire, incapacità di intendere e di volere. Qualora eventualmente cessata la situazione di impedimento si dovrà procedere per il seguito dell'attività di cura a raccogliere il consenso del diretto interessato.

fettuate con o senza l'ausilio di strumenti elettronici, riguardanti 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 di dati.

2. Modalità del trattamento
   a) Titolare del trattamento è (nome e cognome, indirizzo e recapito del titolare se persona fisica, riferimenti, indirizzo della sede e recapiti del titolare se ente).
   b) Il trattamento dei dati è effettuato dal titolare (e/o dal responsabile), tramite il personale sanitario e amministrativo, nonché tramite personale consulente o convenzionato.
   c) Il trattamento è eseguito sia con strumenti manuali che informatico-telematici, comunque con l'osservanza di misure di sicurezza in grado di garantire che solo personale autorizzato possa conoscere le informazioni che riguardano la persona assistita e i suoi familiari e di ridurre al minimo i rischi di perdita, distruzione o accesso non autorizzato ai suoi dati.
   d) In relazione al trattamento eseguito con strumenti informatico-telematici si specifica che tale trattamento potrà essere effettuato con modalità di telemedicina e teleassistenza.
   e) Il trattamento dei dati dell'assistito è necessario per poter effettuare le prestazioni richieste e/o necessarie per la tutela della salute della persona assistita. Il mancato consenso al trattamento dei dati, con l'eccezione dei trattamenti urgenti e di quelli disposti da Autorità Pubblica, potrà comportare l'impossibilità di prestare l'assistenza sanitaria.
   f) Il Responsabile del trattamento è (nome e cognome del responsabile se persona fisica, riferimenti del responsabile se ente).
3. Ambito di comunicazione dei dati
   I dati anagrafici, anamnestici e clinici dell'assistito saranno resi disponibili al personale sanitario, tecnico e amministrativo afferente a (indicare ente, amministrazione, organismo, struttura, dipartimento, area etc che si occuperà del trattamento dei dati) - nei limiti delle competenze di ciascun operatore - per le attività di diagnosi, cura, prevenzione e riabilitazione, nonché per le attività di carattere amministrativo, di controllo di gestione e di rendicontazione.

4. Diritti dell'interessato
   Sono riprodotte di seguito le norme dell'art. 7 della citata legge, che stabiliscono i diritti dell'interessato in relazione al trattamento dei dati personali:

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 del Codice della Privacy;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

CONFERIMENTO DEL CONSENSO

Si precisa che:
il trattamento sarà avviato con il consenso scritto del familiare e previa lettura della presente informativa.

Poiché ai sensi dell'art. art. 82, comma 2, lett.a del Codice della Privacy il consenso al trattamento dei dati è validamente manifestato, in luogo di chi si trova in situazioni di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere, da chi esercita la potestà genitoriale, la tutela ovvero da un familiare, da un prossimo congiunto, da un convivente

il sottoscritto/a _____
nato/a a _____il _____
e residente in_____
in qualità di: _____
(scrivere QUI SOPRA se si è genitore, tutore, congiunto, familiare o convivente dell'assistito)

dichiara di aver preso visione delle informazioni riportate nel documento "INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI" allegato ed esprime altresì il proprio consenso al trattamento e alla comunicazione dei dati personali e sanitari dell'assistito.

Firma di presa visione ed accettazione.

_____

Data _____ Luogo_____

Allegato 7
INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

(D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali")

CONSENSO DEL FAMILIARE AL TRATTAMENTO DEI SUOI DATI[83]

Gentile Familiare,
la presente comunicazione ha lo scopo di informarLa che il decreto legislativo 196/2003 (cd. Codice della Privacy) prevede la tutela dei dati personali, nel pieno rispetto dei diritti e delle libertà fondamentali, oltre che delle norme sul segreto professionale.
Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.
I Suoi dati personali, i Suoi dati sensibili e i Suoi sanitari, ove Lei acconsenta firmando l'apposito modulo che Le verrà consegnato dagli operatori di … (indicare riferimenti del titolare o del responsabile), verranno raccolti per la realizzazione di per …… (indicare l'attività per cui è necessario il trattamento dei dati), come più dettagliatamente spiegato in …… (indicare eventuali allegati che illustrino l'attività), che Le è stata consegnato insieme alla presente informativa.
Ai fini del Codice della Privacy, La si informa di quanto segue:

1. Finalità del trattamento
   I Suoi dati personali, con particolare riferimento a quelli riferiti allo stato di salute, saranno trattati per … (indicare l'attività per cui è necessario il trattamento dei dati).

2. Modalità del trattamento
   Titolare del trattamento è (nome e cognome, indirizzo e recapito del titolare se persona fisica, riferimenti, indirizzo della sede e recapiti del titolare se ente).
   a) Il trattamento dei dati è effettuato direttamente dal titolare (e/o dal responsabile), tramite il personale sanitario e amministrativo, nonché tramite personale consulente o convenzionato.

[83] Un progetto di telemedicina può richiedere, oltre al trattamento dei dati relativi allo stato di salute dell'assistito, anche la raccolta di informazioni sullo stato di salute dei familiari del paziente. A questo fine è stato qui inserito anche un modulo per la raccolta del loro consenso.

b) Il trattamento è eseguito sia con strumenti manuali che informatico-telematici, comunque con l'osservanza di misure di sicurezza in grado di garantire che solo personale autorizzato possa conoscere le informazioni che riguardano la persona assistita e i suoi familiari e di ridurre al minimo i rischi di perdita, distruzione o accesso non autorizzato ai suoi dati.
c) In relazione al trattamento eseguito con strumenti informatico-telematici si specifica che tale trattamento potrà essere effettuato con modalità di telemedicina e teleassistenza.
d) Il trattamento dei Suoi dati è necessario per poter effettuare le prestazioni richieste e/o necessarie per la tutela della sua salute (e/o della persona assistita). Il mancato consenso al trattamento dei dati, con l'eccezione dei trattamenti urgenti e di quelli disposti da Autorità Pubblica, potrà comportare l'impossibilità dello svolgimento della descritta attività.
e) Il Responsabile del trattamento è (nome e cognome del responsabile se persona fisica, riferimenti del responsabile se ente).

3. Ambito di comunicazione dei dati
   l Suoi dati anagrafici, anamnestici e clinici saranno resi disponibili al personale sanitario, tecnico e amministrativo afferente a (indicare ente, amministrazione, organismo, struttura, dipartimento, area etc che si occuperà del trattamento dei dati) - nei limiti delle competenze di ciascun operatore - per le attività di diagnosi, cura, prevenzione e riabilitazione, nonché per le attività di carattere amministrativo, di controllo di gestione e di rendicontazione..

4. Diritti dell'interessato
   Sono riprodotte di seguito le norme dell'art. 7 della citata legge, che stabiliscono i diritti dell'interessato in relazione al trattamento dei dati personali:
   1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
   2. L'interessato ha diritto di ottenere l'indicazione:
      a) dell'origine dei dati personali;
      b) delle finalità e modalità del trattamento;
      c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
      d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 del Codice della Privacy;
      e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in

qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

CONFERIMENTO DEL CONSENSO

Si precisa che:
il trattamento sarà avviato con il consenso scritto dell'interessato e previa lettura della presente informativa.

Il sottoscritto/a _____
nato/a a _____ il _____
e residente in _____

dichiara di aver preso visione delle informazioni riportate nel documento "INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI" allegato ed esprime altresì il proprio consenso al trattamento e alla comunicazione dei propri dati personali e sanitari.

Firma di presa visione ed accettazione.

_____

Data _____ Luogo_____