9. ALLEGATI AL DOCUMENTO DI FATTIBILITÀ

9.1 Strumenti di comunicazione

Gli strumenti per la comunicazione che il Nucleo di Fattibilità ha individuato per la divulgazione a breve termine dei risultati del presente Studio sono relativi alla produzione di un **logo di progetto** e ad una **Conferenza Stampa** congiunta del Ministro della Salute e del Ministro dell'Innovazione e le Tecnologie, alla quale saranno invitati giornalisti nazionali ed esteri.

Il logo di progetto, definito dagli esperti di comunicazione del Nucleo, dovrà essere approvato dai responsabili politici di entrambe le Amministrazioni coinvolte nello Studio di Fattibilità.
La conferenza stampa potrà avere luogo nella sede del Ministero della Salute o del Ministro per l'Innovazione e le Tecnologie, nel prossimo mese di giugno, compatibilmente con gli impegni istituzionali in agenda. Un'ulteriore occasione di divulgazione potrebbe essere individuata nell'ambito degli eventi relativi al Semestre di Presidenza di turno dell'Unione Europea.

La conferenza stampa informerà i cittadini italiani e la comunità scientifica dell'imminente realizzazione della prima rete telematica progettata a supporto di servizi di teleconsulto medico tra i centri sanitari italiani nel mondo e i centri nazionali di riferimento, e che tale servizio sarà operativo a partire dal febbraio del 2004.

Le azioni, quindi, che si intendono promuovere attraverso la conferenza sono:

1. Informare tutte Istituzioni che rappresentano un nucleo di interesse per il progetto stesso: *Ospedali ed aziende sanitarie più importanti, Centri di Ricerca, IRCCS, Società Scientifiche* più rappresentative.

2. Amplificare l'interesse e i contatti tra le Amministrazioni e le *Università*, sia per quanto riguarda le Facoltà di Medicina e Chirurgia, Farmacia e Biologia, che per quanto riguarda le Facoltà di Ingegneria e Informatica.

3. Favorire l'attivazione di *canali di comunicazione e di scambio* con i centri sanitari italiani attualmente non ancora aderenti al progetto.

4. Suscitare l'interesse del mondo produttivo italiano e non, per la creazione di un *partenariato* finanziario e di investimento.

Più in generale, il Nucleo ha individuato alcune opzioni per la futura predisposizione del piano di comunicazione del progetto IPOCM.

Le seguenti indicazioni derivano sia dall'esame degli obiettivi di progetto e delle sue modalità di realizzazione, sia dalla sua rilevanza nel sistema Paese in relazione alla salute pubblica e alle opportunità che potrebbe offrire al sistema industriale:

1. Promuovere il modello di rete integrata, per favorire la nascita di analoghe reti di solidarietà ed aiuto nei Paesi in via di sviluppo, così da poter coinvolgere e aiutare anche la popolazione autoctona.
2. Informare i cittadini italiani dell'esistenza di strutture sanitarie italiane all'estero a cui potersi rivolgere in via privilegiata in caso di necessità.
3. Costruire, curare e rafforzare nel tempo l'immagine della rete.
4. Stimolare il senso di appartenenza al progetto degli operatori delle strutture coinvolte nella rete.
5. Favorire il coinvolgimento attivo nel progetto del personale medico/sanitario già operante nei centri sanitari italiani.
6. Favorire, tra tutti gli attori coinvolti nella rete, la produzione di progetti complessi e condivisi da più strutture, mirati al miglioramento del livello generale delle prestazioni e dei servizi offerti dai centri sanitari italiani nel mondo.
7. Promuovere gli scambi professionali degli operatori del settore.
8. Coinvolgere il mondo universitario e informare il mondo studentesco in genere, attraverso lo sviluppo di progetti di ricerca universitari ed "invogliare" giovani studenti universitari a collaborare con gli ospedali esteri, supportandone anche periodi di studio presso le strutture sanitarie in questione
9. Stimolare l'interesse dei privati (Aziende, Fondazioni, Società) verso il progetto, così da invogliare investimenti nel finanziamento di attività ad esso correlate.
10. Promuovere la solidarietà tra i cittadini nei confronti degli strutture sanitarie italiane nel mondo.
11. Promuovere e rafforzare lo scambio culturale e professionale attraverso l'utilizzo della rete.

Infine, le seguenti quattro tipologie di target di utenza, a cui prioritariamente rivolgere l'azione di comunicazione, possono essere considerate appropriate:

- Popolazione italiana residente in Italia e all'estero (cittadini).
- Operatoti sanitari, medici di base e medici specialisti.
- Docenti universitari, ricercatori, dottorandi e studenti legati all'ambito sanitario.
- Società scientifiche e centri di ricerca scientifica più rappresentativi in Italia.

9.2 Disamina delle norme di riferimento per il progetto

Disposizioni normative antecedenti alla legge n. 675/96

L'attenzione sempre più incisiva per una garanzia piena delle informazioni sulla salute, in Italia, ha trovato una significativa conferma nella *legge n. 675 del 31.12.1996* relativa alla tutela dei **dati personali** (tra i quali, come facilmente comprensibile, quelle informazioni rientrano) che costituisce il primo intervento normativo specifico ed organico in materia di **privacy**.

Prima dell'entrata in vigore di tale legge, infatti, erano rinvenibili solo disposizioni frammentarie o relative a settori ben precisi, riconducibili all'ampio concetto di privacy e disseminate nelle più disparate fonti normative.

Nel definire il quadro normativo della materia che qui interessa occorre, tuttavia, partire proprio dalla nostra Carta Costituzionale in quanto il **diritto alla riservatezza**, e cioè il diritto a non subire intrusioni da parte di terzi nella propria sfera intima attraverso la diffusione di informazioni personali indipendentemente dalla propria volontà, è certamente comprensibile tra i **diritti inviolabili dell'uomo** riconosciuti e garantiti dalla Repubblica ai sensi dell'art. 2 Cost, pur non essendo espressamente menzionato.

In particolare, l'esigenza di tutela del diritto alla riservatezza costituisce la ratio dei principi dell'inviolabilità della libertà personale e del domicilio, della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione, e della libertà nella manifestazione del pensiero (artt. 13, 14, 15, 21 Cost.).

Riguardo, invece, alle altre norme sparse nell'ordinamento giuridico italiano e ricollegabili sempre alla tutela della privacy si citano a mo' di esempio l'art. 10 cod. civ. in materia di diritto all'immagine; gli artt. 622 e 623 cod. pen. che puniscono la rivelazione di **segreti professionali**, scientifici o industriali; l'art. 615-bis cod. pen. che punisce le interferenze nella vita privata mediante la rivelazione o diffusione di notizie ad essa relativa; l'art. 615-quater cod. pen. che punisce la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; la legge 20.05.1970 n. 300 c.d. Statuto dei Lavoratori laddove pone il divieto per il datore di lavoro di violare la privacy dei lavoratori sul luogo di lavoro; etc. etc. (Dati sensibili e soggetti pubblici, Commento sistematico al D. Lgs. 135/1999, di Bisso-DellaTorre-Ferrara-Fidani-Jannelli-Linzola-Miele-Panassidi-Papa-Zucchetti; Giuffrè Editore).
Prendendo spunto da questa elencazione, un discorso che in questa sede merita certamente di essere approfondito è quello pertinente al principio del **segreto professionale** (preesistente al testo normativo-base sulla tutela della privacy) rilevato che la circolazione in rete dei dati sanitari inevitabilmente si scontra con i limiti discendenti dai principi della deontologia medica.
L'*art.622 del codice penale* prima citato, infatti, obbliga i medici, i chirurghi, i farmacisti, le levatrici ed ogni altro esercente la professione sanitaria a tenere segreti i dati sanitari di cui hanno avuto notizia per ragione della loro professione, dati che tali soggetti potranno omettere di svelare nel prestare testimonianza (*art. 351 c.p.p. ed art. 249 c.p.c.*).
L'*attuale Codice deontologico medico all'art.11* introduce già il divieto per i medici di collaborare alla costituzione di banche dati elettroniche se non in presenza di idonee garanzie di tutela della riservatezza, sicurezza e privacy dell'assistito.
Invero, il passaggio dai documenti cartacei a quelli informatici aumenta il rischio di violazione del segreto professionale, potendo questi ultimi documenti essere facilmente manomessi senza che ne rimanga traccia, e, sotto l'aspetto medico legale, costituisce una **trasmissione di segreto professionale lo scambio di dati informatici tra due operatori**.
Detti operatori non saranno necessariamente professionisti sanitari, in quanto, tenuti al rispetto del segreto professionale saranno comunque **tutti gli aventi accesso alle reti telematiche**, compresi per es. gli operatori tecnici ed il personale amministrativo (cfr. Considerazioni medico legali in tema di telemedicina, E. Ricciarello, C. Durante, F. Mangiapane, M. Nucci).
Si osserva, tuttavia, che deve ritenersi esistente una **"giusta causa"** ex art.622 c.p., legittimante quindi la rivelazione delle informazioni sanitarie normalmente coperte dal segreto professionale, ove ricorra **l'esigenza di tutela dell'integrità psicofisica del terzo**.
Quanto appena detto trova infatti conferma all'art. 9 del codice deontologico medico che indica espressamente quale "giusta causa di rivelazione" l'urgenza di salvaguardia della vita o della salute dell'interessato o di un terzo, quando l'interessato non possa prestare il suo consenso per incapacità di agire, di intendere e di volere, o perché fisicamente impossibilitato, nonché l'urgenza di tutela della vita o della salute di terzi, pur in caso di diniego dell'interessato ma con l'autorizzazione del Garante (cfr. Il Diritto alla riservatezza, Antonino Scalisi, Giuffrè Editore).
Si aggiunge che la legge n. 675/96 nell'istituire il Garante per la protezione dei dati personali gli ha attribuito anche il potere di promuovere (art. 31 lett. h), con esplicito riferimento alle attività che comportano il trattamento dei dati inerenti la salute e la vita sessuale (art. 22 comma 4^), la sottoscrizione da parte delle federazioni nazionali degli ordini e dei collegi delle professioni sanitarie di appositi **codici di deontologia e di buona condotta** di cui verificherà, altresì, la legittimità e si impegnerà ad assicurarne la diffusione e l'osservanza (cfr. "Manuale di diritto dell'informatica- Ettore Giannantonio, Vol. 1^ CEDAM").
L'importanza di tale fonte di regolamentazione è stata ribadita dall'*art. 17 del D.Lgs. n. 135/99*, di cui si dirà oltre, emanato ad integrazione della legge n. 675/96, il quale al n.3 pone l'accettazione di siffatto codice quale condizione essenziale per il trattamento dei dati da parte degli incaricati del trattamento stesso, ma, soprattutto, il recentissimo D.Lgs. n. 467 del 28.12.2001 recante disposizioni integrative e correttive della normativa in materia di privacy all'art. 20 ha posto al Garante il termine del **30.06.2002** per la promozione dell'**approvazione del codice** di cui sopra, stabilendo altresì i settori in cui l'adozione di siffatto codice è obbligatoria.
Tornando a delineare il quadro normativo antecedente all'entrata in vigore della legge n. 675/96, occorre precisare che il concetto di dato personale non è un portato della legge appena citata in quanto le **iniziative comunitarie** in materia sono, rispetto al primo intervento normativo organico italiano, risalenti nel tempo:
la *"Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale" del Consiglio d'Europa del 28.01.1981* imponeva già per il trattamento dei **dati sensibili** appropriate garanzie, e la *Raccomandazione della Commissione Europea* volta a promuovere la firma e la ratifica da parte dei paesi membri della citata *Convenzione europea del 1981*, adottava un occhio di riguardo per quest'ultima categoria di dati suggerendone la registrazione in apposite **banche dati** in modo da individuarne gli scopi, il contenuto ed il responsabile della banca, sottolineando altresì la necessità della esattezza ed aggiornamento dei **dati sanitari** nonché della loro conservazione per il tempo strettamente indispensabile.
Si consentiva, inoltre, l'accesso alle **banche dati** riguardanti la salute solo agli esercenti la professione sanitaria per la cura del malato e, in tutti gli altri casi, per fini statistici, di ricerca, didattici, ecc.., con il **consenso** dell'interessato e le **autorizzazioni** previste dal regolamento delle banche dati.
Dal contenuto della Convenzione nasceva, poi, la distinzione tra **due specie** di dati sanitari da tenere separate:
dati sanitari di carattere obiettivo come per es. temperatura, gruppo sanguigno, prescrizioni terapeutiche, ambiente sociale, professione;
dati sanitari di carattere soggettivo come per es. diagnosi probabile, ipotesi di evoluzione di una malattia, comportamento, attitudini;
Ancora più rigida era la posizione adottata nella *Direttiva del 24.10.1995 n. 46/95*, emanata in attuazione dell'accordo di Schengen del 1985, fissandosi il principio del divieto di trattamento derogabile con il consenso dell'interessato oppure, con adeguate garanzie, su iniziativa delle autorità degli Stati membri per motivi di **interesse pubblico rilevante**.
Nella fattispecie, detta *Direttiva n. 46/95*, pur disponendo in ordine a tutti i dati sensibili, evidenziava l'esigenza di dedicare maggiore attenzione alla tutela dei **dati inerenti alla salute** in quanto **"particolarmente sensibili"**, rilevando contemporaneamente che proprio per la loro natura **il trattamento di tali dati deve essere agevole** ed essere consentito agli esercenti la professione sanitaria, ove effettuato **per esigenze terapeutiche o scientifiche**, senza il vincolo del consenso dell'interessato e dell'autorizzazione del Garante.
Quindi, ogni tentativo di disciplina della materia *de qua* vedrà da una parte la necessità di porre dei paletti alla circolazione in rete delle informazioni riguardanti lo stato di salute degli individui, a tutela della loro riservatezza, dall'altra l'esigenza che tali limiti non ostacolino iniziative consentite dalla moderna tecnologia volte alla cura di interessi primari aventi ad oggetto la vita e la salute.

La legge n. 675 del 31.12.1996: "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".
L'esigenza di un intervento legislativo generale ed organico in materia di tutela della privacy, che desse attuazione alla Direttiva n. 46/95 di cui sopra e colmasse un vuoto normativo particolarmente avvertito in seguito al rapido diffondersi delle tecnologie informatiche, ha trovato finalmente riscontro nell'approvazione della legge n. 675 del 31.12.1996 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", entrata in vigore l'08.05.1997.
Premesso che in questa sede se ne illustreranno soltanto gli articoli aventi una qualche rilevanza per la tutela dei dati sanitari, si rileva che tale legge è stata successivamente integrata e modificata con numerosi atti normativi di cui si dirà, tra i quali spiccano il recentissimo D. Lgs. 28.12.2001 n.467, e, nella materia che qui interessa il D. Lgs. n.135 dell'11.05.1999 sul trattamento dei dati sensibili da parte dei soggetti pubblici, nonché il D. Lgs. n. 282 del 30.07.1999 recante disposizioni per garantire la riservatezza dei dati personali in ambito sanitario.

Innanzitutto, va chiarito che **finalità** della legge n. 675/96, come precisato all'art.1 comma 1^, è quella di garantire il pieno rispetto dei diritti, delle libertà fondamentali, e della dignità dell'individuo, "*con particolare riferimento alla riservatezza ed all'identità personale*", nel trattamento dei dati personali.

Dato personale

Ai sensi dell'art.1 comma 2^ lett. c) legge citata, con il termine **"dato personale"** si intende ogni informazione relativa ad un soggetto **identificato** o **identificabile** (cosiddetto **interessato**, v. lett. f) comma cit.) sia esso persona fisica, persona giuridica, ente od associazione.
Dalla lettera i) dello stesso comma si trae, invece, che il dato è definibile **anonimo** laddove non possa essere associato ad un soggetto identificato o anche indirettamente identificabile.
Come si vede, il concetto di dato personale fornito dalla legge è abbastanza ampio abbracciando qualsiasi elemento di conoscenza in ordine a fatti o stati dell'individuo, qualunque ne sia la forma e la connotazione.
Importante poi è la presa di posizione del legislatore italiano nell'estendere la tutela a soggettività diverse dalla persona fisica, considerato come l'argomento non è affatto pacifico in sede comunitaria ed internazionale tant'è che la Convenzione Europea del 1981 e la Direttiva Comunitaria n. 46/95 hanno semplicemente attribuito agli stati membri la possibilità di detta estensione.

Trattamento dati

Ma cosa deve intendersi esattamente per "**trattamento dei dati**"?
L'art. 1 comma 2^ lett. b) ne da una definizione abbastanza ampia, comprensiva in generale di ogni attività di identificazione, elaborazione, e circolazione dei dati, precisando nel dettaglio che il trattamento consiste in "*qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio dei mezzi elettronici o comunque automatizzati, concernente 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, la distruzione dei dati*".
Tuttavia, va subito precisato che presupposto per l'applicazione della legge non è la singola operazione di trattamento bensì l'esistenza di una **banca dati** definita, infatti, dalla legge prima di qualsiasi altra delle nozioni esposte alla lett. a) del comma 2^ come "*qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento*".
Perché ci sia una banca dati è quindi sufficiente la presenza di un insieme di dati personali, indipendentemente dalle modalità di raccolta ed organizzazione di essi, potendo essa constare di un archivio **cartaceo** o **informatizzato**, come sempre più spesso accade.
Altri due concetti di rilievo definiti sempre dall'art. 1 comma 2^ alle lettere g) ed h) che appare utile esporre sono quelli, apparentemente simili, di **comunicazione** e **diffusione** dei dati personali le cui modalità la legge disciplina successivamente agli artt. 20 e 21.
Mentre la comunicazione consiste nel dare conoscenza dei dati a uno o più **soggetti determinati** diversi dall'interessato con qualsiasi forma, anche attraverso la semplice messa a disposizione o consultazione (ad es. invio di una lettera ad un destinatario ben preciso), la diffusione consiste nel dare conoscenza dei dati a **soggetti indeterminati**, ad una pluralità indistinta di soggetti, anche qui indipendentemente dalla forma utilizzata (ad es. pubblicazione di una notizia in un quotidiano).
(cfr. Il Diritto alla riservatezza, Antonino Scalisi, Giuffrè Editore; Dati sensibili e soggetti pubblici, Commento sistematico al D.Lgs. n.135/1999, di Bisso-DellaTorre-Ferrara-Fidani-Jannelli-Linzola-Miele-Panassidi-Papa-Zucchetti; Giuffrè Editore).

Figure chiave

Anticipando che l'argomento verrà approfondito nella seconda parte del presente lavoro, attraverso l'individuazione in concreto degli accorgimenti pratici da adottare in attuazione delle norme qui di seguito esposte, appare opportuno rilevare sin d'ora che, al fine di rendere operativa la disciplina in essa contenuta, la legge n. 675/96 definisce tre figure chiave deputate a perseguire le finalità di tutela della privacy:
1.**Il titolare del trattamento dei dati personali**; trattasi della persona fisica, della persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo, dotati del potere di prendere le decisioni fondamentali in ordine alle finalità ed alle modalità del trattamento, e dunque sulla raccolta e l'utilizzazione dei dati, anche sotto il profilo della sicurezza (lett. d) comma 2^).
Quella appena descritta è, pertanto, una figura obbligatoria su cui grava tutta la responsabilità giuridica discendente dal trattamento e dagli obblighi connessi sottolineando che, come chiarito dal Garante (figura che si va a descrivere in prosieguo), nell'ambito di un'amministrazione pubblica, di una società o di un ente, il titolare è da individuare nella struttura complessivamente intesa e non nella persona fisica che lo rappresenta o amministra.
2.**Il responsabile del trattamento**; trattasi del soggetto (persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo) preposto dal titolare al trattamento dei dati, fornito di qualità che lo rendano idoneo a garantire il rispetto delle prescrizioni normative in materia di trattamento, e sottoposto al rispetto delle istruzioni impartite nello stesso atto di nomina ed al controllo del titolare (lett. e) comma 2^ art. 1 ed art. 8 legge cit.).
A differenza del titolare, la figura del responsabile del trattamento è facoltativa perché laddove non si provveda alla sua nomina, che potrà oltretutto riguardare anche un soggetto esterno all'ente, entrambe le qualifiche si concentreranno in capo al primo.
Seppure, invece, il titolare nomini il responsabile ciò non lo esime da responsabilità potendosi configurare, in merito all'operato della persona prescelta, la sua culpa *in eligendo* e *in vigilando*.
Inoltre, come l'art. 8 comma 3^ suggerisce, nelle aziende e negli enti di dimensioni medio-grandi in cui si tengono più banche dati e con contenuti differenti, è opportuno procedere alla nomina di un responsabile per ciascuna banca.
3.**L'incaricato del trattamento;** in assenza di una precisa definizione di legge ma come si evince dall'art.8 ultimo comma e dall'art.19, tale è la persona fisica che materialmente elabora i dati personali, per es. l'operatore del computer, a cui è fatto obbligo di seguire le istruzioni del titolare o del responsabile, soggetti questi ultimi che vigileranno sul suo operato.
Proprio a questa figura, come si vedrà nella seconda parte di questo lavoro, sono dirette una serie di prescrizioni contenute nel citato DPR n. 318/1999 ed aventi ad oggetto le misure di sicurezza che in concreto dovranno essere adottate nel trattamento.

Ufficio del Garante

A vigilare su tutto il complesso sistema di tutela dei dati personali voluto dalla legge sarà l'ufficio del **Garante per la protezione dei dati personali** istituito dalla stessa legge n. 675/96, che vi accenna già all'art. 1 comma 2^ lett. m), e vi dedica poi gli artt. 30 e ss Capo VIII.
Questo ufficio costituisce un'autorità amministrativa indipendente, operante infatti ai sensi del comma 2^ dell'art. 30 in piena autonomia e con indipendenza di giudizio e di valutazione, ed avente composizione collegiale.
Numerosi sono i compiti ed i poteri attribuiti dalla legge alla figura del Garante e riconducibili sinteticamente alla tenuta del **registro generale dei trattamenti**, ad attività di **controllo** e vigilanza sul rispetto delle prescrizioni di legge esercitate d'ufficio o su iniziativa dei terzi, di **stimolo** (si pensi alla promozione dei codici deontologici cui si accennava) ed **informazione** (es. diffusione della conoscenza delle norme sulla privacy), di **tutela** (attraverso le decisione dei ricorsi presentati dagli interessati che si ritengono violati nella privacy), di **consulenza** (anche nei confronti del Parlamento); il Garante, poi, è rivestito di due importanti **poteri** che sono quello **sanzionatorio** (irrogazione di sanzioni amministrative per colpire le violazioni della legge n. 675/96) e quello **autorizzatorio,** esplicantesi nel rilascio di autorizzazioni **individuali** al trattamento nei casi in cui la legge

lo richieda (vedi *infra* per la materia che qui interessa), e di autorizzazioni **generali** relative a determinate categorie di titolari o di trattamenti ed introdotte da una fonte normativa successiva alla legge in esame (vedi *infra*).

Ambito di applicazione
Anche l'ambito di applicazione della normativa in essa contenuta è ben individuato dalla legge n. 675/96 che all'art. 2 lo estende al "*trattamento di dati personali da chiunque effettuato nel territorio dello Stato"*, nonché al trattamento operato fuori dall'Unione Europea ma con mezzi situati nello Stato, ed in quest'ultimo caso il titolare dovrà designare un rappresentante stabilito nel territorio italiano.

Aspetti applicativi
La **notificazione**, il cui obbligo è previsto all'art. 7, si configura come l'atto fondamentale di legittimazione della banca dati e delle operazioni di trattamento in quanto, il titolare che intenda procedere a trattamento rientrante nel campo di applicazione della legge sulla privacy, ne deve dare comunicazione preventiva al Garante nelle forme prescritte "*se il trattamento, in ragione delle relative modalità o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato"*.
Analoga comunicazione preventiva deve essere effettuata in caso di cessazione, per qualsiasi causa, del trattamento, cosi come deve darsi comunicazione delle eventuali modifiche intervenute.
La notificazione deve contenere una serie di dati, espressamente indicati sub art. 7, c. 4°, della legge 675/96, finalizzati a fornire un'informativa sufficientemente completa ed esaustiva in ordine al trattamento che il titolare intende effettuare.
Quando il trattamento è effettuato da enti pubblici sulla base di espressa disposizione di legge o di apposito provvedimento del Garante, è prevista una forma di notificazione semplificata caratterizzata dalla riduzione delle informazioni da fornire al Garante, rispetto a quanto richiesto in via ordinaria (art. 7,c. 5 bis, legge 675/96, nonché D.lgs. n. 467/01) .

La **raccolta dei dati e la loro registrazione** (che in realtà può considerarsi la forma nella quale la raccolta avviene) devono essere effettuate secondo i criteri stabiliti all'art. 9 c. 1° della legge in esame, ed in particolare:
i dati personali "*devono essere raccolti e registrati per scopi determinati, espliciti e legittimi"* che i privati nel creare una banca dati dovranno preventivamente delimitare mentre, nel caso di enti pubblici, tali finalità potranno essere definite per legge (lett. b);
i dati devono essere "***esatti**, se necessario **aggiornati, pertinenti, completi**, e non eccedenti le **finalità** per le quali sono raccolti o successivamente trattati":* qualità tutte riempibili di contenuto sempre in relazione allo scopo della raccolta (lett. c e d);
i dati raccolti devono essere trattati in modo **lecito** (in conformità alla normativa sulla privacy ed a tutte le altre norme rilevanti in materia) e **corretto** (e cioè nel rispetto delle regole imposte soprattutto dai codici deontologici, dalle consuetudini informatiche, ed in genere proprie del "buon gestore dei dati" (lett. a);
i dati personali, infine, devono essere conservati in maniera tale da rendere identificabile l'interessato fino al momento in cui sono raggiunti gli scopi della raccolta e del trattamento e non oltre, sottolineando così l'importanza del principio della finalità (lett. e).
Si può derogare, tuttavia, al limite temporale di cui sopra nel caso in cui il trattamento avvenga per scopi storici, di ricerca scientifica, o di statistica (comma 1 bis dello stesso art. 9).

L'informativa all'interessato, disposta dall'art. 10 è una delle prescrizioni di carattere pratico più rilevanti, che deve essere effettuata come primo adempimento quando si inizia un'attività di trattamento di dati personali.
Ciò al fine di mettere al corrente, oralmente o per iscritto, la persona cui i dati si riferiscono circa le caratteristiche del trattamento ed i diritti che vanta informandola, in particolare, delle finalità e modalità del trattamento, dei soggetti ai quali i dati possono essere comunicati e dell'ambito di diffusione dei dati medesimi, dei dati identificativi del responsabile del trattamento, nonché della posizione che l'interessato stesso riveste rispetto al trattamento.
In quest'ultimo caso, si fa riferimento alle informazioni sulla natura obbligatoria o facoltativa del conferimento dei dati, sulle conseguenze di un eventuale rifiuto, ed infine sul diritto di accesso e diritti connessi che l'interessato vanta.
Oltre che in ipotesi tassativamente contemplate, anche nella materia che qui interessa, tuttavia, l'informativa può essere prestata in forma semplificata, laddove provenga da organismi sanitari pubblici nonché da organismi sanitari ed esercenti professioni sanitarie convenzionati o accreditati dal Servizio Sanitario Nazionale, nelle forme che un apposito decreto del Ministro della Sanità dovrà fissare nel dettaglio e che, in generale, vedranno l'informativa provenire da un unico soggetto, cioè **il medico generale** scelto dall'interessato, per conto di più titolari del trattamento, e la possibilità di fornire le informazioni dopo la richiesta della prestazione nei **casi di urgenza**.
Chiarito che l'obbligo dell'informativa riguarda anche i **soggetti pubblici**, se il trattamento da parte loro riguarda i **dati sensibili** (di cui *infra* e tra i quali rientrano i dati sanitari) occorrerà avvisare, altresì, l'interessato della normativa che prevede gli obblighi o i compiti per i quali il trattamento avviene.

Il consenso previsto dall'art.11 è il principio fondamentale in materia di dati personali. In linea generale l'esistenza del consenso subordina il trattamento dei dati da parte di privati ed enti pubblici
Il consenso deve essere:
relativo all'intero trattamento o ad una o più sue operazioni (comma 2^);
espresso liberamente, dunque consapevole e non implicito, in forma specifica e per iscritto;
informato, cioè preceduto dall'informativa di cui si è detto (comma 3^).
L'art. 12 contempla, invece, i casi di esclusione del consenso tra i quali particolare importanza presentano, per quanto in questa sede interessa, quelli di cui alle lettere d) e g):
caso di trattamento finalizzato unicamente a scopi di ricerca scientifica o di statistica, nel rispetto dei codici di deontologia di cui all'art. 25 cit.;
caso di trattamento necessario per la **salvaguardia della vita o dell'incolumità fisica** dell'interessato o di un terzo, ove l'interessato non possa prestare il proprio consenso per impossibilità fisica, incapacità di agire, di intendere o di volere.
A questo ultimo proposito, il Garante ha avuto modo di precisare che **in campo sanitario**, al fine di snellire gli adempimenti previsti dalla legge, il consenso può essere acquisito dal medico *una tantum*, in relazione al complesso delle attività poste in essere nei confronti dei propri assistiti.
Un altro caso di esclusione del consenso che merita di essere menzionato, introdotto dal D.Lgs. n. 467/01 in nome del principio del bilanciamento di interessi, è quello di cui alla lettera h) bis del cit. art 12 il cui portato attribuisce al Garante il potere di individuare altri casi di esclusione "*sulla base dei principi della legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato"*.

Diritti dell'interessato
Come si accennava nella parte relativa all'informativa, l'interessato vanta una serie di diritti rispetto al trattamento dei suoi dati che gli consentono l'esercizio di un potere di controllo sulla legittimità delle operazioni, ed infatti la legge prevede all'art.13:

un diritto di conoscenza, consistente nella facoltà per l'interessato di accedere gratuitamente al registro dei trattamenti e delle notificazioni ricevute dal Garante per verificare l'esistenza di trattamenti che lo riguardano, e conoscerne quindi modalità e finalità, nonché il responsabile ed il titolare (lett. a) e b);
un diritto definibile di accesso, esercitatile nei confronti stavolta del responsabile o del titolare, i quali, saranno tenuti senza ritardo ad informare l'interessato dell'esistenza o meno di dati che lo riguardano, con comunicazione degli stessi dati e della loro origine, della logica e delle finalità del trattamento;
un diritto alla correzione dei dati ed in particolare, alla cancellazione, trasformazione in forma anonima, aggiornamento, rettificazione, integrazione dei dati, al blocco dei dati trattati illegittimamente;
un diritto di opposizione per motivi legittimi al trattamento dei propri dati, anche se pertinenti allo scopo della raccolta, con specifico riferimento al trattamento per fini di informazione commerciale;
L'art. 14, tuttavia, contempla alcune ipotesi in cui i diritti elencati non possono essere esercitati e relative soprattutto al trattamento da parte di soggetti pubblici, a salvaguardia di un interesse pubblico al trattamento dei dati, a cui si aggiunge un nuovo caso di esclusione degli stessi diritti introdotto dal D.Lgs. n. 467/01 cit., limitatamente ai dati personali identificativi di chiamate telefoniche entranti, e nei confronti di fornitori di servizi di telecomunicazioni accessibili al pubblico "*salvo che possa derivarne pregiudizio per lo svolgimento delle investigazioni difensive nei procedimenti penali*" (lett. e-bis).

Misure di sicurezza
Affinché le finalità di tutela oggetto del testo di legge in esame possano davvero trovare attuazione, l'art. 15 pone per i soggetti che a vario livello operano il trattamento di dati personali (responsabile, titolare ed incaricati del trattamento), l'obbligo di adottare idonee misure di sicurezza volte, in particolare, a ridurre il cosiddetto rischio informatico, e cioè ad impedire l'accesso ai dati non autorizzato, la perdita e la distruzione dei dati, un trattamento non consentito o non autorizzato dalla legge.
Per tali fini, i dati personali dovranno essere custoditi e controllati in relazione alla loro natura, alle caratteristiche del trattamento, ed al progresso tecnico.
Si precisa che il comma 2^ dell'art. 15, demanda l'individuazione in concreto e nel dettaglio delle misure di sicurezza a successivo regolamento, ed in attuazione a ciò è stato emanato il DPR del 28.07.1999 n. 318 che ci si riserva di approfondire nella seconda parte del capitolo.

Modalità di comunicazione e diffusione
Avendone già fornito le nozioni nella parte introduttiva, la legge, poi, agli artt. 20 e ss. disciplina nel dettaglio le modalità con le quali la **comunicazione** e la **diffusione** dei dati devono avvenire, distinguendo a seconda che il trattamento avvenga da parte di **privati o enti pubblici economici** (art.20) o da parte di **soggetti pubblici** (art.27).
In linea di principio può dirsi che per i primi, comunicazione e diffusione dei dati sono permesse laddove la legge e l'interessato lo consentano rilevando, per quanto qui interessa, la previsione della lett. f) dell'art. 20 cit. secondo la quale i soggetti diversi da quelli pubblici potranno comunque procedere alla comunicazione ed alla diffusione se "*necessarie per la **salvaguardia della vita o dell'incolumità fisica** dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere*".
L'art. 21 nel porre i divieti di comunicazione e diffusione dei dati personali, tuttavia, al comma 4^ lett. a) ammette in ogni caso tali operazioni divulgative quando necessarie per finalità di **ricerca scientifica** o di statistica, nel rispetto dei **codici deontologici e di buona condotta** di cui si è detto.
Quanto ai soggetti pubblici, premettendo che l'argomento verrà approfondito nella seconda parte esaminando il testo del *D.Lgs. 11.05.1999 n. 135*, specificatamente dedicato al trattamento da parte di soggetti pubblici dei dati sensibili, compresi quelli sanitari, in linea di massima si può dire che la legge n. 675/96 ammette il trattamento dei dati personali senza la necessità del consenso dell'interessato, ma soltanto "*per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti*".

Dati sensibili
L'art. 22 distingue dai dati personali comuni una particolare categoria di dati personali definiti "sensibili", relativi agli aspetti più intimi della persona, ed esattamente consistenti in quelli "*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*".
Ai sensi del citato art. 22, i dati sensibili possono essere oggetto di trattamento, da parte dei soggetti privati o degli enti pubblici economici, solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.
Sarà comunque sufficiente la sola autorizzazione del Garante, secondo quanto stabilito al comma 4^ dell'art. 22 cit., laddove il trattamento sia necessario "*per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere*" (lett. b), oppure per lo svolgimento delle investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto, di rango pari a quello dell'interessato, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale (lett. c).
Inoltre, sempre per il *favor* nei confronti dell'interessato, ai sensi del comma 2^ art. 22 , la mancata comunicazione entro 30 giorni al titolare del trattamento della decisione adottata dal Garante, equivale a rigetto dell'istanza volta ad ottenere l'autorizzazione.
I **soggetti pubblici**, invece, ai sensi del comma 3^ art. 22 possono procedere al trattamento dei dati sensibili "*solo se autorizzato da espressa disposizione di legge che specifichi i dati che si possono trattare, le operazioni eseguibili, le rilevanti finalità di interesse pubblico perseguite*" indipendentemente, dunque, dal consenso dell'interessato e dall'autorizzazione del Garante.
Sul trattamento dei dati sensibili da parte degli enti pubblici viene comunque dedicato successivo specifico paragrafo cui si rinvia.

Disposizioni successive alla legge n. 675 del 31.12.1996 in sede nazionale, comunitaria, ed internazionale
Per i motivi prima accennati, l'esigenza di una disciplina rigorosa per il trattamento di dati sensibili si pone in particolare modo per i **dati sanitari**, inerenti alla salute e alla vita sessuale dell'uomo, la cui diffusione può determinare odiose discriminazioni sociali e limitare la libertà dell'individuo, soprattutto in seguito alla ormai frequente formazione di grandi banche dati sanitarie.
Da qui una serie di iniziative adottate a livello internazionale, al fine di porre un freno all'indiscriminata circolazione di informazioni relative alla salute degli uomini:
Numerose sono state poi le iniziative adottate fuori dall'Italia e riguardanti, nel dettaglio, l'incontenibile flusso di **informazioni sulla salute** degli individui attraverso un canale certamente privilegiato quanto alla facilità di accesso e cioè **Internet**:
- Ed invero, abbastanza specifiche sono le prescrizioni che il Comitato dei Ministri del Consiglio d'Europa ha emanato in data 13.02.1997 con la *Raccomandazione n. 5*-97, relativa proprio alla **"Protezione dei dati sanitari" su Internet**.

Tale Raccomandazione ha disposto che nella raccolta e nel trattamento dei dati medici occorre garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla riservatezza, ed a tal fine fissa una serie di linee guida non solo per gli utenti, ma pure per i fornitori di servizi su Internet, da inserire nei codici deontologici o allegarvele, applicabili a tutte le autostrade informatiche.
In particolare, la raccolta ed il trattamento dei dati devono essere effettuati in modo lecito, corretto e per fini determinati, garantendone l'integrità e la segretezza, non permettendo quindi alcuna interferenza nel contenuto delle comunicazioni, informando infine gli utenti dei rischi per la privacy insiti nell'uso di Internet.
Pur ribadendo il principio del consenso, la Raccomandazione citata vi ha posto delle deroghe attuabili in presenza di **interessi pubblici rilevanti**: a tutela della sanità pubblica o per la prevenzione e repressione dei reati (art. 4.3a); per fini di prevenzione, terapeutici o diagnostici, per la tutela di interessi vitali dell'interessato o di terzi, per l'adempimento di un'obbligazione contrattuale ed infine per l'accertamento, l'esercizio, e la tutela di un diritto soggettivo (art.4.3b).
(Cfr. "Manuale di diritto dell'informatica-Ettore Giannantonio, Vol. 1^ CEDAM").
- Nel 1999 il Consiglio d'Europa ha promulgato alcune *linee guida riguardo alla privacy su Internet*, da inserire o allegare ai codici deontologici e, più di recente, l'Unione Europea per competere nella Società dell'Informazione, seppure in ritardo rispetto agli USA ed al Giappone, ha varato *un programma per la "e.Europe"* volto a favorire lo sviluppo di servizi tecnologicamente avanzati, infatti uno degli obiettivi decennali del programma prevede che ogni cittadino, azienda ed Amministrazione Europea siano connessi in Rete con una priorità: la **Sanità on-line**, ovvero lo sviluppo di reti telematiche per migliorare l'assistenza sanitaria ai cittadini.
- Nel tentativo di frenare la circolazione incontrollata in rete di informazioni sanitarie, la Commissione Europea ha sponsorizzato la creazione dell' *"Health on the Net (HON) Foundation"*, organizzazione *non profit* per lo sviluppo e la diffusione di nuove tecnologie dell'informazione in medicina con sede in Ginevra, la quale ha promulgato nel 1996 *un codice di condotta (autoregolamentazione) per i siti sanitari*, emesso in 11 lingue italiano compreso e divenuto, oramai, lo **standard di riferimento internazionale al momento più diffuso ed accreditato sul Web,** soprattutto perché offre all'utente la possibilità di valutare se il sito è stato realizzato con requisiti minimi qualitativi.
- Ed un altro codice etico molto dettagliato è *l' "e. health code of ethics"*, riguardante tutto il popolo di Internet in Sanità, ed i cui principi guida sono: chiarezza, onestà, qualità (=accuratezza), consenso informato, **privacy**, professionalità, partnering responsabile, accreditamento (certezza dell'interlocutore e qualità dei servizi).
Si tratta di un codice promulgato dall'*Internet Healthcare Coalition* in accordo con l'AMA (*American Medical Association*), l'*Health Internet Ethics Group*, e l'HON (*Health On Net Foundation)* organizzazione, quest'ultima, sponsorizzata dalla Commissione Europea.
- Infine, nel 1998 l'Organizzazione Mondiale della Sanità ha lanciato l'*Health Telematic Policy* ed ha pubblicato una **guida** in sei punti **all'uso di Internet in sanità** che evidenzia i vantaggi del reperimento facile e veloce di informazioni utili (diagnosi, terapie, organizzazioni, enti e servizi sanitari) da utilizzare sempre col supporto del medico curante.
(Cfr. Internet e salute, Aspetti etico sociali formativi normativi e regolamentari, Dott. R. Maceratini dell'A.S.M.I.).
In ambito nazionale, per arginare il rischio di facili ingerenze da parte di terzi nel flusso telematico di informazioni sanitarie, il legislatore italiano è più volte intervenuto dettando norme volte ad assicurare la riservatezza e la sicurezza degli individui in ordine al trattamento di dati inerenti alla loro salute, norme che si vanno brevemente ad illustrare riservandosi di approfondirne successivamente i risvolti pratici.
Per temperare il rigore delle prescrizioni in materia di cui alla legge n. 675/96, la cui applicazione comporterebbe, di volta in volta, la necessità di procurarsi nei casi stabiliti l'autorizzazione del Garante, è stato emanato il *decreto legislativo n. 123 del 09.05.1997* che attribuisce al Garante per la protezione dei dati personali la possibilità di rilasciare le cosiddette **autorizzazioni generali** relative, cioè, a determinate categorie di titolari o di trattamenti, ed autorizzazioni di questo tipo (a cui si ritornerà in seguito) sono state emanate finora con scadenza annuale, senza sostanziali modifiche, in attesa di un intervento legislativo in materia.
Specificatamente al trattamento da parte di soggetti pubblici dei dati sensibili, compresi quelli sanitari, è dedicato il citato *D.Lgs. 11.05.1999 n. 135* il quale, oltre ad individuare per il settore sanitario alcune attività da considerare di interesse pubblico e nell'ambito delle quali, quindi, è consentito il trattamento dei dati inerenti la salute, prevede l'uso di **apposite misure** a tutela della riservatezza dell'interessato come **la cifratura, i codici identificativi,** ecc...
Ed ulteriori prescrizioni in tal senso sono altresì contenute nel successivo *DPR del 28.07.1999 n. 318*, riguardante i dati personali in generale oltre che i dati sensibili, ma soprattutto, per la materia che qui interessa, nel *D.Lgs del 30.07.1999 n. 282* recante appunto *"Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"*.
Quest'ultimo decreto ha apportato modifiche ed integrazioni alla legge n. 675/96 specie in materia di informativa e consenso, ha disposto in merito a due precise tipologie di documenti quali le **prescrizioni mediche** e le **carte sanitarie elettroniche**, ed all'art. 5 contiene un'interessante deroga al principio del consenso per il caso in cui il trattamento dei dati idonei a rilevare lo stato di salute sia finalizzato a **scopi di ricerca scientifica** in campo medico, biomedico o epidemiologico, effettuata in attuazione a norme di legge o nell'ambito del programma di ricerca biomedica o sanitaria di cui al *D.Lgs. del 30.12.1992 n. 502*.
La giungla di disposizioni normative nella quale gli operatori sanitari devono districarsi è arricchita anche dai numerosi *decreti emessi dal Garante* tra i quali emerge quello *del 09.11.2000* rivolto a **tutti i medici** con archivi cartacei, computer isolati o collegati in rete, che registrano **dati sensibili**, ai quali si prescrive l'adozione di una serie di provvedimenti per impedire che tali dati vadano persi o che vi possa accedere personale non autorizzato. Si precisa che **la violazione** di tali disposizioni è **perseguibile penalmente** (Notizie di Maggio 2001, Sito Internet della Federazione Italiana Medici di famiglia, Sezione Provinciale di Caltanissetta).
Inoltre, particolare rilevanza assume il *DPR del 28.12.2000 n. 445 recante il "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"* il quale definisce i concetti di **documento informatico** e **firma digitale**: il primo è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; la firma digitale, invece, consiste in una procedura elettronica (c.d. validazione) di attestazione della provenienza dell'atto e di garanzia dell'integrità del suo contenuto, basata su un sistema di chiavi asimmetriche a coppia.
Le disposizioni concernenti i concetti appena esposti trovano applicazione non solo nel **settore pubblico** ma anche **nei rapporti tra privati** (art. 2 DPR n. 445/2000), con la precisazione che il documento informatico e la firma digitale avranno comunque la valenza probatoria e l'efficacia giuridica che nello stesso DPR vi si attribuisce.
La sezione III del capo II di quest'ultimo DPR, poi, tratta anche della **trasmissione del documento informatico**, non trascurando di considerare il problema della **riservatezza dei dati personali** contenuti e della **segretezza della corrispondenza** trasmessa per via telematica, disciplinando altresì al capo IV l'**accesso al sistema** di gestione informatica dei documenti.
L'autorizzazione generale del Garante in materia di trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale (l'ultima è la *n. 2/2002* pubblicata in G.U. del 09.04.2002) ha previsto una disciplina differenziata per gli esercenti una professione sanitaria e gli organismi sanitari pubblici, autorizzati in linea di massima a trattare i dati anche senza il consenso dell'interessato per fini di tutela dell'incolumità fisica e della salute di un terzo o della collettività, e per gli organismi e le case di cura private, che possono invece procedere al trattamento solo ed esclusivamente in presenza del consenso scritto dell'interessato.
Questo è punto molto discusso è sicuramente di notevole impatto per i progetti di telemedicina, ovvero è necessario il consenso informato per il trattamento dei dati in regime di telemedicina da parte dell'interessato?

Sia l'art.32 della Costituzione italiana, secondo il quale "nessuno può essere obbligato ad un determinato trattamento sanitario se non per disposizione di legge", sia la Legge n.833/78 con le successive modificazioni sanciscono il diritto del paziente alla scelta dei professionisti e dei **luoghi** ove venire curati. Se ne evince pertanto che il paziente deve prestare il proprio consenso al particolare trattamento, pur riconoscendo la libertà del medico di consigliare ed indirizzare verso la competenza migliore.
Per il trattamento dei dati sensibili sanitari, la legge n.675/96 sulla "privacy" prevede che le PA possano esimersi dal raccogliere il consenso informato. Ciò purché esista una legge o un regolamento che definisca i dati da trattare, le modalità e le finalità del trattamento stesso. Normativa specifica non è stata emanata e le Aziende Sanitarie non hanno potestà regolamentare a rilevanza esterna. Pertanto si deve ritenere che le strutture sanitarie pubbliche siano comunque tenute alla informativa (art.10 della Legge n.675/96) e alla raccolta del consenso scritto del paziente (art.11 della legge n.675/96), per svolgere tutte le attività di trattamento dei dati rilevanti nell'esecuzione delle prestazioni mediche.
Conseguentemente si evince che debba sempre essere prestato dal paziente interessato anche un consenso informato specifico per il trattamento dei dati sensibili sanitari trasmessi in regime di teleradiologia.

Decreto del Presidente della Repubblica 28 luglio 1999, n.318
Successivamente alla legge 675 è stato emanato un DPR n.318/99 dal titolo "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675". In tale DPR si definiscono alcuni principi fondamentali quali:
"**misure minime**": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;
"**strumenti**": i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
"amministratori di sistema": i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.
Oltre a queste definizioni vengono chiariti due diversi ambiti operativi: il trattamento mediante elaboratori non accessibili a rete pubblica e quello mediante elaboratori accessibili alla rete pubblica. Per il progetto in esame si può sicuramente individuare la seconda possibilità in quanto per lo scambio dei dati clinici si utilizzeranno reti pubbliche quali quelle di Internet. Per questo tipo di trattamento devono essere adottate le seguenti misure:
a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale
Un aspetto fondamentale è la definizione del cosiddetto "Documento programmatico sulla sicurezza". Infatti nel caso di trattamento dei dati personali deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:
a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.
L'efficacia delle misure di sicurezza adottate deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

9.3 Questionario per l'acquisizione delle informazioni tecniche dai centri sanitari nel mondo

Guida alla compilazione del **QUESTIONARIO** per l'acquisizione delle informazioni tecniche -Progetto IPOCM-

Il presente Questionario tecnico ha lo scopo di acquisire i dati relativi alla situazione delle telecomunicazioni in essere presso la Vostra struttura sanitaria, nonché la disponibilità, interna alla struttura, di una postazione di lavoro (hardware e software) destinabile al progetto IPOCM.

Tale acquisizione di informazioni renderà possibile l'individuazione dei bisogni di ciascuna struttura, e sarà tanto più rispondente alla realtà quanto più accurata sarà la risposta della struttura al presente questionario.

Il questionario si rivolge ai responsabili delle telecomunicazioni e dei sistemi informatici della struttura sanitaria, e richiede, eventualmente, la consultazione dei contratti di acquisto o locazione.

Vi prego di barrare le caselle di scelta, così come di prestare attenzione alla legenda sotto riportata, che chiarisce l'ambito di alcune domande contenute nel questionario.

Vi ringrazio sentitamente per la collaborazione e Vi auguro buona compilazione!

Dr. Gianfranco Costanzo

Responsabile del progetto IPOCM

Legenda delle note

1. Grado di soddisfazione dell'utente sul servizio offerto dal gestore internazionale.
2. Quante volte è necessario ricomporre il numero telefonico per riuscire ad ultimare la chiamata.
3. Rumori di fondo o inserimenti di altre conversazioni.

QUESTIONARIO
per l'acquisizione delle informazioni tecniche

PARTE I: Informazioni generali sulle TLC ☒

A. Fonia fissa

1. Linee analogiche dirette n°..... uso fonia ☐ uso fonia e dati ☐ uso dati ☐
2. Linee digitali ISDN n°..... uso fonia ☐ uso fonia e dati ☐ uso dati ☐
3. Linee digitali xDSL n°.....
4. Fax SI ☐ NO ☐ / Telex SI ☐ NO ☐
5. Centralino telefonico SI ☐ NO ☐
   - Se si: Marca.....Modello.....n° Linee su centralino.....
6. Qualità del servizio percepita[1] dall'utente su una scala da 1(pessima) a 5 (ottima) .....
7. Cadute di linea[2] n°..... Interferenze[3] SI ☐ NO ☐
8. Società telefonica fornitrice: ragione sociale.....

   indirizzo.....

   nome e tel. del referente.....

B. Fonia mobile

1. Telefoni cellulari in servizio SI ☐ NO ☐
   - Se si: uso fonia ☐ uso fonia e dati ☐
2. Società telefonica fornitrice: ragione sociale.....

   indirizzo.....

   nome e tel. del referente.....
3. Qualità del servizio percepita[1] dall'utente su una scala da 1(pessima) a 5 (ottima) .....
4. Cadute di linea[2] n°..... Interferenze[3] SI ☐ NO ☐
5. Fornitori presenti a livello nazionale: ragione sociale.....

   indirizzo.....

C. Trasmissioni satellitari

1. Esistenza nella struttura di Trasmissione ☐ Ricezione ☐ Trasm/ricez. ☐
2. Fornitore del servizio: ragione sociale.....
   indirizzo.....
3. Fornitore presente sul territorio: ragione sociale.....
   indirizzo.....

D. Internet

1. Connessione Internet Service Provider (ISP) SI ☐ NO ☐
   - Se si: ISP fornitore ragione sociale.....
     indirizzo.....
     collegamento via modem: velocità .....Kb/s
     collegamento su linea ISDN: SI ☐ NO ☐ BRI:.....PRI:.....
     collegamento su linea ADSL: SI ☐ NO ☐ Velocità effettiva.....Kb/s
     collegamento su linea HDSL: SI ☐ NO ☐ Velocità effettiva.....Kb/s
2. Qualità del servizio percepita[1] dall'utente su una scala da 1(pessima) a 5 (ottima) .....
3. Cadute di connessione: SI ☐ NO ☐
4. Tempo medio di attesa collegamento < 1 minuto ☐ > 1 minuto ☐
5. Servizio IP contrattualizzato[4]: Disponibilità %.....
   Velocità di accesso Kb .....
   Banda garantita Kb.....
   - Se no: ISP presenti sul territorio: ragione sociale.....
     indirizzo.....

PARTE II: Strumenti e applicazioni

E. Hardware

1. Disponibilità di PC da impiegare nel progetto SI ☐ NO ☐
   - Se si: Caratteristiche microprocessore: < Pentium II o equiv. ☐ > Pentium II ☐
     RAM < = 64 Mb ☐ > 64 Mb ☐
     Hdisk < = 10 Gb ☐ > 10 Gb ☐
     Monitor b/n ☐ colore ☐
     Scheda audio SI ☐ NO ☐
     Tipo scheda video:.....
2. Caratteristiche delle periferiche
   Scanner: b/n ☐ colore ☐ A3 ☐ A4 ☐
   Lettore CD: SI ☐ NO ☐ DVD: SI ☐ NO ☐

F. Software

- Sistema operativo: Microsoft DOS ☐ Microsoft Windows ☐ Apple ☐
  System x ☐ Unix SI ☐ NO ☐
  Linux SI ☐ NO ☐
- Software operativo: e-mail SI ☐ NO ☐ ftp client SI ☐ NO ☐
  Browser: Microsoft Explorer rel. .....
  Netscape rel. .....
  Altro .....

G. Altro

- Sistema di videoconferenza SI ☐ NO ☐
- Se presente una collaborazione con Centri sanitari in Italia, ciò avviene con:
  Internet ☐ telefono ☐ altro ☐
  Per scopi di:
  Teleconsulto ☐ formazione ☐ informazione ☐
- E' presente nella struttura una postazione DICOM? SI ☐ NO ☐

9.4 Questionari per l'acquisizione delle informazioni tecniche dagli ISP

GUIDA PER LA COMPILAZIONE DEL QUESTIONARIO

QUESTIONNAIRE FILLING IN GUIDE

Il presente questionario è indirizzato ai fornitori di servizi internet (ISP) dei centri sanitari italiani nel mondo.

Il Ministero della Salute italiano sta elaborando uno studio di fattibilità per il collegamento in rete dei centri sanitari italiani nel mondo che hanno aderito agli obiettivi di uno specifico progetto per la loro connessione, materiale e immateriale, con centri sanitari sul territorio nazionale e con il Ministero della Salute italiano (vedere progetto IPOCM su www.ministerosalute.it).

Verrebbe così creata una rete mondiale di centri sanitari italiani, sulla quale veicolare prestazioni sanitarie in telemedicina ed eventi formativi a distanza, sia per il personale medico che per quello sanitario, con lo scopo finale di innalzare il livello qualitativo delle prestazioni sanitarie.

Si prega di voler compilare il presente questionario entro il 5 dicembre, in italiano o in inglese, e di volerlo restituire allo scrivente, al seguente indirizzo di posta elettronica: g.costanzo@sanita.it

Si ringrazia per la cortese collaborazione.

Dr. Gianfranco Costanzo
Responsabile progetto IPOCM

The following questionnaire is addressed to the Internet Service Providers for the Italian health care centres world-wide.

The Italian Ministry of health is carrying out a feasibility study to connect via web the Italian health care centres world-wide endorsing the objectives of an "ad hoc" project for their material and virtual connection to Italian health care centres on the national territory and to the Italian Ministry of Health (see IPOCM project on www.ministerosalute.it).

By doing so we expect to obtain a world-wide web of Italian health care centres, through which addressing both diagnosis and cures by telemedicine and distance learning events to medical and health personnel, with the final aim of improving the quality of health care.

You are kindly asked to fill in the attached questionnaire by December 5th, either in English or in Italian, and send it back to the following e-mail address: g.costanzo@sanita.it

Thank you for your cooperation.

Dr. Gianfranco Costanzo
Responsible for IPOCM project

QUESTIONNAIRE FOR INTERNET SERVICE PROVIDERS

SECTION I – Identification data

Name of enterprise.....

Brand.....

Mother group.....

Address.....

Z.I.P..... City.....

State..... Phone number.....

Fax number..... e-mail.....

Internet site..... Company capital $.....

Name of administrative account manager .....

Phone ..... e-mail.....

Name of technical account manager .....

Phone ..... e-mail.....

Geographic market areas.....

Kind of enterprise: Network provider ☐ ISP ☐ ASP ☐

SECTION II – Services provided on the basis of kind of enterprise

a) Network Provider

services provided:

Connectivity	YES ☐	NO ☐
Voice	YES ☐	NO ☐
Streaming:	YES ☐	NO ☐
Unicast	YES ☐	NO ☐
Multicast	YES ☐	NO ☐
Videoconference	YES ☐	NO ☐

Nucleo Interministeriale per la Fattibilità della Rete IPOCM

Other (describe).....

Added value services:

Backup	YES ☐	NO ☐
Network management	YES ☐	NO ☐
Security	YES ☐	NO ☐

Other (describe).....

Technology:

ADSL	YES ☐	NO ☐
HDSL	YES ☐	NO ☐
DSL	YES ☐	NO ☐
ATM	YES ☐	NO ☐
Frame Relay	YES ☐	NO ☐
Satellite	YES ☐	NO ☐
Wireless	YES ☐	NO ☐
Wi-fi	YES ☐	NO ☐

Other (describe).....

Other information:

Backbone in use (describe).....

Services on re-sale (describe).....

Number of customers:

residential customers N.....

small enterprises N.....

medium enterprises N.....

large enterprises N.....

b) Internet Service Provider (ISP)

Access services:

IP best effort YES ☐ NO ☐
- Standard availability % .....
- Access speed kb/s .....

IP with quality of service (QoS) YES ☐ NO ☐
- Standard availability % .....
- Access speed kb/s .....
- Guaranteed band kb/s .....

IP multicast YES ☐ NO ☐
- Standard availability % .....
- Access speed kb/s .....
- Guaranteed band kb/s .....

Final user's access technology:

Switched line

PSTN	YES ☐	NO ☐
ISDN	YES ☐	NO ☐

Leased line

ADSL	YES ☐	NO ☐
HDSL	YES ☐	NO ☐
DSL	YES ☐	NO ☐
Satellite	YES ☐	NO ☐
Wi-fi	YES ☐	NO ☐
Wireless	YES ☐	NO ☐

Multicast protocols

DVMRA	YES ☐	NO ☐
MOSPF	YES ☐	NO ☐
PIM-SM	YES ☐	NO ☐

Nucleo Interministeriale per la Fattibilità della Rete IPOCM

Other (describe).....

Neutral Access Point (NAP) connection

Domestic YES ☐ NO ☐

International YES ☐ NO ☐

Access band to NAP kb/s .....

c) Application service provider (ASP)

Services:

Provision of standard applications YES ☐ NO ☐

- If yes, which ones?.....

Housing/hosting YES ☐ NO ☐

System integration YES ☐ NO ☐

Other (describe).....

Interest in IPOCM project YES ☐ NO ☐

Please, attach your prise list

9.5 Lettere di approfondimento per gli ISP

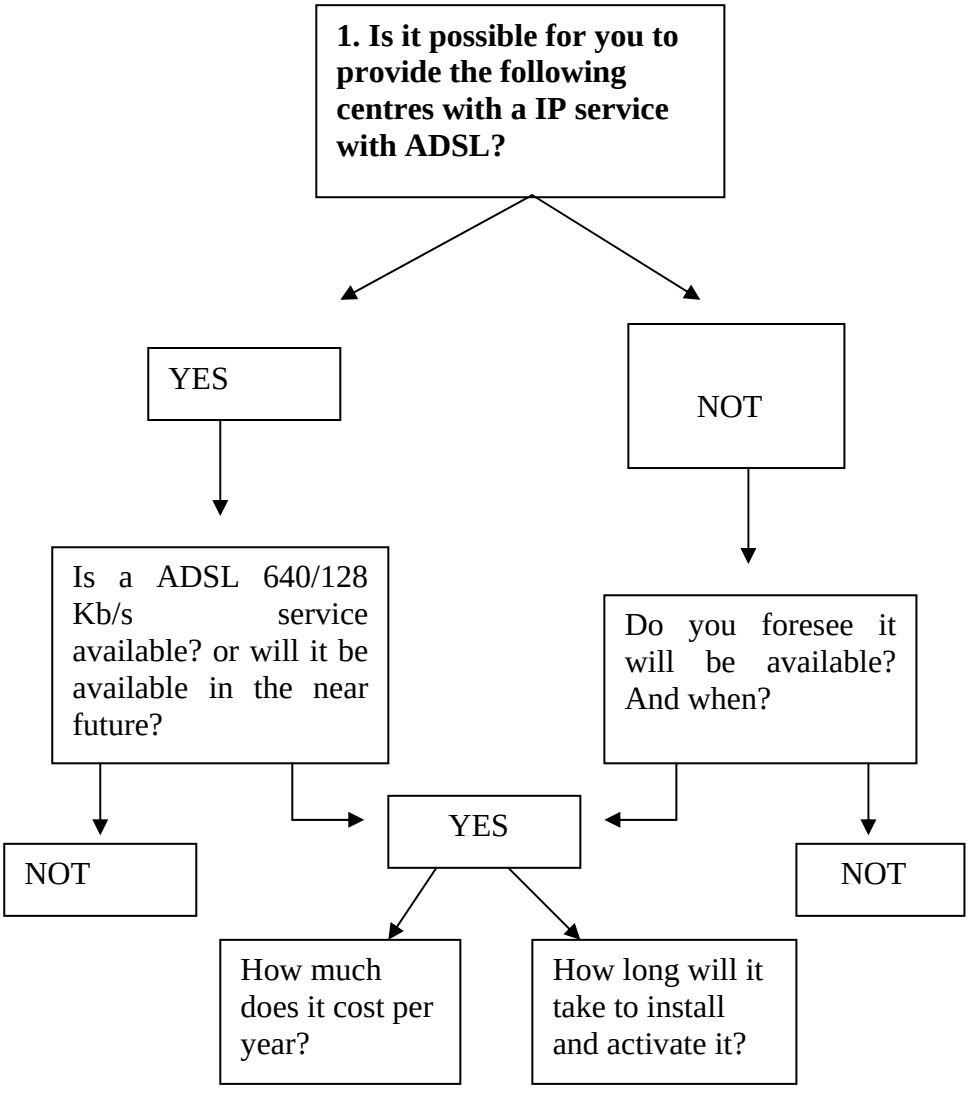
Dear Mr. ……..,

You have already filled in an information questionnaire sent out by the Italian Ministry of Foreign Affairs regarding an Italian project aiming at connecting Italian hospitals worldwide each other and with Italian health structures on the national territory.

We would like to thank you for that fruitful cooperation which has given us the possibility to step on forward the production of a feasibility study of the telematic network amongst Italian hospitals abroad.

In order to acquire as precise information as possible, we are now asking your further cooperation on the following three issues:

1. ADSL



2. HDSL - ISDN

2. Is it possible for you to provide the following centres with IP service with HDSL 1Mb/512 Kb/s and/or ISDN?

- If yes, how much will it cost per year?
- If not, how long will it take to install and activate it?

3. SECURITY SERVICES

3. Can you provide security services, namely firewalling, VPN and IPSEC?

- If yes, could you indicate their price?

With regard to the hospital listed below, please do check its hospital's address and answer the appropriate questions.

XYZ

Your answer will serve to define, where appropriate, within 2003, a possible contract with you in ADSL or HDSL.

In conclusion, I would like to thank you again for the effort you have done and you will assure in the near future.

Yours sincerely

Dr. Gianfranco Costanzo

Country	Name of Hospital	ADSL			ADSL 640/128 Kb/s		
		Time[1]	Price	Date[2]	Time[1]	Price	Date[2]
			$			$	

Country	Name of Hospital	HDSL 1Mb/512Kb/s			ISDN		
		Time[1]	Price	Date[2]	Time[1]	Price	Date[2]
			$			$	

Country	Name of Hospital	PRICE		
		Firewalling	VPN	IPSEC
		$	$	$

9.6 Decreto istitutivo del Nucleo Interministeriale per la fattibilità della rete IPOCM

MOD. 5 - U.G.

Ministero della Salute

Dipartimento per la Tutela della Salute Umana Sanità Pubblica Veterinaria e Rapporti Internazionali

IL MINISTRO

VISTO il Progetto per l'Integrazione e la promozione degli Ospedali Italiani e dei Centri di Cura con Assistenza Italiana nel Mondo, denominato progetto IPOCM;

VISTO il cronoprogramma del progetto IPOCM che prevede, tra l'altro, uno studio di fattibilità per la rete degli ospedali italiani nel mondo;

VISTA la sottoscrizione dell'Atto di Adesione agli obiettivi del progetto IPOCM avvenuta a Roma il 28 ottobre 2002 nel corso della Prima Conferenza per l'Integrazione e Promozione degli Ospedali Italiani nel Mondo;

CONSIDERATA la volontà espressa, nel corso della suindicata Prima Conferenza di Roma, da parte dei responsabili del Ministero per gli Italiani nel Mondo, del Ministero degli Affari Esteri, del Dipartimento per l'Innovazione e le Tecnologie, e del Rappresentante del Presidente del Consiglio dei Ministri in seno al G8 per i Paesi dell'Africa, di procedere, con ogni sollecitudine, all'attuazione delle fasi previste dal progetto IPOCM, avvalendosi anche delle risorse in essere presso dette Amministrazioni centrali;

VISTO l'art. 18 della Legge 28 dicembre 2001 n° 448, recante disposizioni per la formazione del bilancio annuale e pluriennale dello Stato;

PRESO ATTO che, per la natura dei compiti da affidare, non è possibile l'utilizzazione esclusiva di proprio personale, atteso che non sono presenti, tra gli appartenenti a questa amministrazione, tutte le professionalità occorrenti al raggiungimento delle summenzionate finalità,

DECRETA

Art. 1

In ordine allo svolgimento delle attività di pianificazione e studio della fattibilità della rete degli ospedali italiani nel mondo, è istituito, presso il Dipartimento per la Tutela della Salute Umana, della Sanità Pubblica Veterinarie e dei Rapporti Internazionali, il *Nucleo Interministeriale per la Fattibilità della Rete del Progetto IPOCM* , d'ora in avanti chiamato Nucleo.

MINISTERO DELLA SALUTE
Dipartimento II
17 FEB. 2003
Prot. 21/489

Art. 2

Il Nucleo opererà nel periodo di tempo dedicato alla fattibilità della rete del progetto IPOCM e, comunque, non oltre il 30 maggio 2003.

Art. 3

Il Nucleo è costituito da:

1. Dr. Gianfranco COSTANZO, in rappresentanza della D.G. dei Rapporti Internazionali e delle Politiche Comunitarie, con funzioni di coordinatore;
2. Dr.ssa Manuela COCCHI, in rappresentanza della D.G. dei Rapporti Internazionali e delle Politiche Comunitarie;
3. Dr. Alfredo D'ARI, in rappresentanza della D.G. degli Studi, della Documentazione Sanitaria e della Comunicazione ai Cittadini;
4. Dr.ssa Lidia DI MINCO, in rappresentanza della D.G. del Sistema Informativo e Statistico e degli Investimenti Strutturali e Tecnologici;
5. Ing. Giovanna EUSEPI, in rappresentanza del Ministro per l'Innovazione e le Tecnologie;
6. Dr.ssa Paola MONARI, in rappresentanza del Ministro per l'Innovazione e le Tecnologie;
7. Sig.ra Francesca PASCUCCI, in rappresentanza del Dipartimento per l'Innovazione e le Tecnologie per le Comunicazioni Esterne.
8. Dr.ssa Rosa ROSINI, in rappresentanza della D.G. del Sistema Informativo e Statistico e degli Investimenti Strutturali e Tecnologici

Art. 4

Il Nucleo potrà avvalersi di esperti di settore per gli approfondimenti tecnici richiesti dallo studio di fattibilità.

Il presente decreto sarà trasmesso agli organi di controllo secondo la normativa vigente.

Roma, li 11 FEB. 2003

IL MINISTRO