ALLEGATO D

Breve manuale sulle cautele da adottare nel trattamento di dati personali.

Alle persone che entrano in contatto con medici e strutture sanitarie per cure, prestazioni mediche, acquisto di medicine, operazioni amministrative, devono essere garantite la più assoluta riservatezza ed il rispetto della dignità.
I dati personali in grado di rivelare lo stato di salute delle persone sono infatti di particolare delicatezza, per questo definiti “dati sensibili”, e non possono essere diffusi.
Ad essi il Codice sulla protezione dei dati personali attribuisce una tutela rafforzata e stabilisce le regole per il loro trattamento in ambito sanitario, tenendo sempre conto del ruolo professionale dei medici e del personale paramedico.
Questo breve manuale tenta di offrire un quadro delle principali indicazioni fornite dal Garante nel corso del tempo. L’intento dichiarato è di agevolare le attività degli operatori e di contribuire a migliorare le condizioni di vita quotidiana di chi accede a qualunque luogo di analisi o cura.

E’ opportuno evidenziare che nessuna guida operativa, per quanto dettagliata, potrà mai sostituire le intuizioni dettate dal buon senso e dal rispetto della dignità umana, valori certamente permeanti la personalità di tutti coloro che hanno scelto di lavorare in ambito sanitario.

Ogni definizione utilizzata è ripresa dal D.L.vo 196/03 (Codice della Privacy).

L’articolo 30, comma 1 del D.L.vo 196/03 prevede che le operazioni di trattamento dei dati personali possono essere svolte solo da incaricati, che operano sotto la diretta autorità del Titolare o del Responsabile.

Titolare del trattamento, secondo quanto previsto dall’art. 28 del codice della privacy, è l’ I.R.C.C.S. - ISTITUTO NAZIONALE PER LO STUDIO E LA CURA DEI TUMORI “FONDAZIONE GIOVANNI PASCALE” in persona del suo legale rappresentante pro-tempore.

I TERMINI MAGGIORMENTE USATI:

TRATTAMENTO DEI DATI PERSONALI: qualunque operazione effettuata sui dati, ad esempio, la raccolta, la registrazione, la conservazione, l'elaborazione, l'estrazione, la modificazione, l'utilizzo, la diffusione, la cancellazione etc;

DATO PERSONALE: qualunque informazione relativa ad una persona;

DATO SENSIBILE: qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale dell'interessato;
INTERESSATO: la persona cui si riferiscono i dati personali;

INFORMATIVA: contiene le informazioni che il Titolare del trattamento (ad es. Ospedale, medico, etc.) deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è tenuto a fornire o meno i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati ed in che modo si possono esercitare i diritti riconosciuti dalla legge.

CONSENSO: autorizzazione al trattamento dei propri dati personali rilasciata dall'interessato;

FASCICOLO SANITARIO ELETTRONICO (Fse):
E' il documento elettronico che contiene i dati sanitari di ogni paziente, quali patologie, interventi chirurgici, esami clinici, farmaci prescritti, documentazione relativa ai ricoveri. E' consultabile on line sia dall'interessato, sia da altri soggetti eventualmente autorizzati. E' aggiornabile da medici, farmacisti, Enti ospedalieri;

SOCIAL NETWORK:
I social network (Facebook, Twitter e altri) sono "piazze virtuali", cioè dei luoghi in cui via internet ci si ritrova portando con sé e condividendo on line fotografie, filmati, pensieri, indirizzi di amici e tante altre informazioni;

Di seguito vengono riportate una serie di regole e di istruzioni, che devono essere osservate da ciascuna persona fisica preposta allo svolgimento delle operazioni di trattamento:

a) istruzioni per lo svolgimento delle operazioni caratterizzanti il processo di trattamento:

- **raccolta**:
prima di procedere alla raccolta dei dati personali, ai sensi dell'art. 13 del Codice Privacy, deve essere fornita **l'informativa all'interessato** o alla persona presso cui si raccolgono i dati, (sarà cura del Titolare decidere le modalità per adempiere a questo obbligo);

occorre **procedere alla raccolta dei dati con la massima cura,** verificandone l'esattezza, la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento in conformità a quanto previsto dalla legge e dai regolamenti, seguendo le istruzioni del Responsabile della Struttura di appartenenza (Responsabile del trattamento);

- **registrazione**:
non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;

- **conservazione**:
i documenti o gli atti che contengono dati sensibili o giudiziari devono essere conservati in archivi ad accesso controllato. E' quindi necessario garantire che armadi, schedari e contenitori siano muniti di serratura o che l'incaricato del trattamento, che riceva cittadini e utenti, sia sempre presente nella propria stanza o luogo di lavoro avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura di ciascun Responsabile del trattamento adottare i provvedimenti necessari affinché venga escluso un accesso ad archivi ed a dati da parte di soggetti che non siano incaricati del trattamento;

- **utilizzo**:
i dati possono essere utilizzati solo da coloro che sono stati espressamente incaricati al trattamento. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi, avendo cura di evitare un utilizzo per scopi che non coincidano o che non siano compatibili con quelli istituzionali dell'Istituto in riferimento alle attività affidate e di competenza dell'unità di trattamento di appartenenza;

- **blocco**:
questa operazione può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinata direttamente dal Garante per la protezione dei dati personali;

-comunicazione:
con tale espressione, secondo quanto previsto dalla legge, si intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Ciò che caratterizza l'operazione di comunicazione è il fatto che, considerato il rapporto diretto tra Titolare (**Istituto Fondazione G. Pascale**) ed interessato (ad esempio un cittadino utente, un dipendente o un'impresa), un soggetto determinato (in posizione di terzietà rispetto a questo rapporto bilaterale) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;

- **comunicazione di dati cd**. **comuni:**
qualora il richiedente i dati personali sia un soggetto pubblico, la comunicazione dei cd. dati comuni potrà avvenire, pur in mancanza di espressa previsione di legge o di regolamento, qualora sia necessaria per l'esercizio di una delle finalità istituzionali dell'Ente destinatario della stessa comunicazione. In tal caso, tuttavia, occorrerà segnalare la circostanza al proprio Responsabile in modo che possa procedere alla comunicazione preventiva al Garante per la protezione dei dati personali;

- **comunicazione di dati sensibili:**
i dati sensibili possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge che autorizzi tale operazione in conformità al parere del Garante per la protezione dei dati personali;

- **diffusione**:
per diffusione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". La pubblicazione di qualsiasi atto (all'albo pretorio, in una bacheca o in Internet) che contenga dati personali costituisce, ai sensi del Codice della Privacy, una forma di diffusione di informazioni personali. *(l'art. 22, comma 8 del Codice Privacy vieta espressamente la diffusione di dati personali idonei a rivelare lo stato di salute);*

b) istruzioni per il corretto utilizzo degli strumenti per il trattamento:

- **computer:**
tutte le volte che si abbandona la propria postazione di lavoro si deve aver cura di porre il pc/terminale in condizione da rendere i dati non accessibili ad estranei non autorizzati. (potrebbe ad es. essere utilizzato uno *screen saver* con password o potrebbe essere sospesa la propria sessione di lavoro disconnettendosi dall'applicazione in uso);

- **e-mail ed uso di Internet:**
la posta elettronica deve essere utilizzata per scopi di ufficio. Si ricorda che qualunque comunicazione ricevuta o spedita utilizzando l'indirizzo di posta della Struttura non è corrispondenza personale dell'operatore, per cui potrebbero essere effettuati controlli remoti al fine di verificare l'uso improprio o illecito degli strumenti forniti in dotazione.
Occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti dati sensibili. In tal caso, occorrerà proteggere il contenuto del file dall'accesso e dalla visione di soggetti non autorizzati o non legittimati al trattamento diversi dai destinatari delle comunicazioni elettroniche considerate.
A titolo meramente esemplificativo, si consiglia (a seconda dei casi, da valutarsi a cura del Responsabile del trattamento) il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero all'utilizzo di codici identificativi dell'identità dell'interessato associati ai dati sensibili e giudiziari, in modo da rendere non comprensibili i dati nel caso di intercettazione delle comunicazioni;

- **file di log:** per ragioni di sicurezza, si può avere la necessità di installare dispositivi automatizzati di registrazione delle operazioni svolte con elaboratori elettronici (cd. file di log) ovvero delle connessioni a Internet o dell'uso della posta elettronica;

- **fax:** questo strumento appare utile a garantire efficienza, economicità e velocità di comunicazione, tuttavia, presenta rischi specifici riguardo all'identità (a volte sconosciuta) di colui che materialmente riceve il documento trasmesso.
A tal proposito, prima di inviare documenti contenenti dati sensibili o per i quali vi siano particolari esigenze di riservatezza, è doveroso assicurarsi preventivamente che l'effettivo destinatario sia sul posto per riceverlo o che comunque non vi siano rischi di conoscenza del contenuto da parte di soggetti non autorizzati.

Sarebbe una corretta modalità di invio anticipare telefonicamente la trasmissione avendo cura di inserire in calce alla copertina del fax, che viene utilizzata per la spedizione della documentazione allegata, la seguente formula: *"Qualora il destinatario del presente fax non sia la persona indicata, è pregato di dare immediata comunicazione al mittente a mezzo telefono o fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta con l'avvertimento che in caso di non ottemperanza al presente invito si potrebbe essere ritenuti responsabili della mancanza di protezione e/o dell'uso non autorizzato delle informazioni erroneamente acquisite"*;

- **telefono:**
è assolutamente necessario non fornire per mezzo telefono dati ed informazioni di carattere sanitario o di natura comunque riservata qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante.
Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere identità e qualità dell'interlocutore al fine di richiamarlo successivamente per avere certezza sulla identità;

- **scanner**:
coloro che provvedono all'acquisizione in formato digitale della documentazione cartacea devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati;

- **supporti informatici** (**floppy-disk/cd-rom):**
i supporti informatici già utilizzati per il trattamento di dati sensibili e giudiziari possono essere riutilizzati solo nel caso in cui le informazioni precedentemente contenute non siano più in alcun modo recuperabili, in caso contrario devono essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

- **spedizione di documenti contenenti dati personali a mezzo posta:**
la documentazione contenente dati sensibili o giudiziari deve essere trasferita, anche all'interno dell'Istituto, in busta chiusa, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti.
Per dare garanzia della non apertura della busta e della integrità del contenuto sarebbe opportuno che i lembi della busta fossero sigillati e firmati.
In alternativa è comunque opportuno piegare il documento spillandone i lati;

- **uso di software:**
è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte dell'amministratore di sistema. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito, sia di natura penale che civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal D.Lgs. 518/1992 e successive modificazioni e integrazioni. Tale divieto è necessario al fine di scongiurare il rischio di scaricare programmi appositamente collocati nel web ed atti al furto di dati.

Ulteriori istruzioni per gli incaricati del trattamento con gestione di rapporti di front-office e gestione di documenti cartacei.

- **identificazione dell'interessato**:
in alcuni casi per soddisfare esigenze di verifica dell'identità della persona e garanzia di correttezza del dato da raccogliere può essere necessario identificare il soggetto interessato ed è, pertanto, opportuno richiedere un documento di identità o di riconoscimento;

- **controllo dell'esattezza del dato:**
fare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati facendo il possibile per evitare errori di battitura che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:**
l'incaricato del trattamento ha l'obbligo della riservatezza e del segreto sulle informazioni delle quali venga a conoscenza nel corso delle operazioni di trattamento; deve evitare la comunicazione o la diffusione delle informazioni a soggetti non autorizzati o che non abbiano necessità di conoscere i dati trattati.
Si ricorda che l'eventuale violazione degli obblighi ivi considerati può comportare l'applicazione di sanzioni di natura disciplinare e configura una responsabilità civile e penale secondo quanto previsto dal Codice della privacy;

- **tenuta cartelle e fascicoli:**
qualora si ricevano nella propria stanza utenti e cittadini e si tengano sulla propria scrivania cartelle e fascicoli, si consiglia di fare attenzione a rivoltare le cartelle o di inserire (a seconda delle necessità operative e organizzative) sul frontespizio delle stesse dati ed informazioni che non permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento;

- **distruzione delle copie cartacee**:
è necessario prima di gettare la documentazione nel cestino della carta provvedere a renderne non comprensibile il contenuto. Al fine di realizzare il predetto scopo potranno essere utilizzati apparati distruggi documenti o altri più banali accorgimenti come ad esempio lo strappo dei documenti, la separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc;

Istruzioni in tema di sicurezza degli strumenti elettronici

a) password:
deve essere assegnata a ciascun incaricato, composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
deve essere autonomamente cambiata dall'incaricato ogni sei mesi (nel caso di trattamento di dati personali comuni) ovvero con cadenza trimestrale (per il trattamento di dati sensibili o giudiziari);
non deve contenere riferimenti agevolmente riconducibili all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto.

L'incaricato, nello scegliere la propria password, deve preferibilmente utilizzare anche caratteri speciali e lettere maiuscole e minuscole e deve avere cura di custodirla con la massima attenzione e segretezza senza comunicarla a terzi, essendo, tra l'altro, responsabile di ogni utilizzo indebito o non consentito della stessa.
Qualora si ravvisi la necessità di garantire la disponibilità dei dati e dei documenti a persone terze, deve essere richiesta l'abilitazione all'amministratore di sistema e ogni incaricato deve poter accedere con la propria credenziale di autenticazione;

b) **back-up:**
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere, con cadenza almeno settimanale, alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati a disposizione per poi consegnare i supporti contenenti le copie di salvataggio al soggetto nominato ed incaricato della conservazione. In alternativa riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) **antivirus:**
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi almeno con cadenza settimanale o allorquando venga segnalata dal sistema tale esigenza; inoltre, una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare l'eventuale presenza di virus sull'elaboratore;

d) **conservazione supporti rimovibili:**
i supporti utilizzati per la memorizzazione di copie di file di documenti di lavoro non devono essere lasciati in luoghi accessibili. Si consiglia di riporre cd-rom, floppy disk e dispositivi di memorizzazione in cassetti muniti di serratura ovvero di custodire gli stessi in modo da garantire un accesso controllato.

DOMANDE FREQUENTI:

1) IL PAZIENTE INFORMATO:

Occorre chiedere il consenso al paziente prima di acquisire ed utilizzare informazioni sulla sua salute?
SI. Gli organismi sanitari pubblici come pure gli esercenti le professioni sanitarie devono fornire al paziente una informativa sul trattamento dei dati personali che lo riguardano ed acquisire il consenso al loro uso.

…….e se il paziente non è in grado di dare il consenso al trattamento dei dati, ma deve essere sottoposto a cure?
Non è necessario dare un previo consenso all'uso dei dati nei casi di rischio imminente per la salute, o quando vi è impossibilità fisica o incapacità di agire, di intendere o di volere del paziente. In questi casi il consenso al trattamento dei dati personali può essere espresso, se ne è in grado, dal paziente stesso, successivamente alla prestazione sanitaria ricevuta, o da un terzo (ad esempio un familiare, un convivente, un responsabile della struttura presso cui dimora).

Quali informazioni devono essere fornite al paziente?
L'informativa data all'interessato deve indicare chi è il soggetto (ad es. il medico) che raccoglie i suoi dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e se il paziente è obbligato o meno a fornirli. Deve contenere anche le indicazioni sulle modalità con cui la persona interessata può esercitare i diritti riconosciuti dalla legge, come la richiesta di integrazione, aggiornamento o cancellazione dei dati trattati.

L'informativa deve essere sempre fornita in forma scritta?
NO, l'informativa può essere data una tantum anche oralmente. E' comunque preferibile che venga fornita per iscritto, magari attraverso un pieghevole, oppure affiggendone il testo in un luogo facilmente visibile, come nella sala d'attesa dell'ambulatorio.

2) INFORMAZIONI SULLA SALUTE:

Può il medico informare altre persone sullo stato di salute di un suo assistito?
E' possibile, ma il paziente deve aver indicato a chi desidera che siano fornite tali informazioni.

Se una persona viene portata al pronto soccorso o ricoverata chi può avere notizie?
L'organismo sanitario può dare informazioni, anche per telefono, sulla presenza di una persona al pronto soccorso o sui degenti presenti nei reparti solo ai terzi legittimati, come parenti, familiari, conviventi, conoscenti, personale volontario. L'interessato, se cosciente e capace, deve essere preventivamente informato (ad esempio al momento dell'accettazione) e poter decidere a chi possono essere comunicate notizie sulla propria salute. Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.

Le associazioni di volontariato possono ricevere informazioni sui loro assistiti?
Si, ma devono osservare tutte le regole che le strutture sanitarie prevedono per il proprio personale interno al fine di garantire il rispetto della dignità della persona ed il massimo livello di tutela dei pazienti, nonché il segreto professionale.

L'esito delle analisi o le cartelle cliniche da chi possono essere ritirati?
I referti diagnostici, le cartelle cliniche, i risultati delle analisi ed i certificati rilasciati dagli organismi sanitari possono essere consegnati in busta chiusa anche a persone diverse dai diretti interessati purchè munite di delega scritta.

E' possibile conoscere i dati contenuti nella cartella clinica di un defunto?
Può accedere ai dati personali del defunto chi abbia un interesse proprio, o agisca a tutela della persona deceduta o per ragioni familiari meritevoli di protezione.

3) IN ATTESA

A che serve la distanza di cortesia?
Per garantire la riservatezza dei colloqui. Presso gli sportelli di Ospedali devono essere previsti appositi spazi - spesso segnalati con una riga gialla - oltre i quali gli utenti possano attendere il proprio turno.

Nelle sale d'aspetto in che modo il paziente deve essere informato del proprio turno?
Nei locali di grandi strutture sanitarie i nomi dei pazienti in attesa di una prestazione o di documentazione (ad esempio delle analisi cliniche) non devono essere divulgati ad alta voce. Occorre adottare soluzioni alternative: ad esempio, attribuendo un codice alfanumerico al momento della prenotazione o della accettazione.

All'ingresso dei reparti possono essere affisse le liste dei pazienti in attesa di un interevento?
NO. Non è giustificata l'affissione di liste di pazienti in attesa di intervento in locali aperti al pubblico, con o senza la descrizione della patologia sofferta. Non devono essere visibili ad estranei neanche documenti sulle condizioni cliniche del malato, come le cartelle infermieristiche poste vicino al letto di degenza.

Quali precauzioni deve adottare il personale sanitario per tutelare la privacy dei pazienti?
Il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate. Il Garante ha prescritto a questo scopo specifici accorgimenti per garantire la riservatezza dei pazienti sia durante l'orario di visita, sia all'atto della prescrizione di ricette mediche o del rilascio dei certificati. Tra questi accorgimenti va ricordato, ad esempio, l'uso di paraventi o simili nei reparti di rianimazione volti a limitare la visibilità del malato ai soli familiari e conoscenti.

4) LA SALUTE DEI DIPENDENTI

Il datore di lavoro può chiedere che nei certificati medici sia indicata la diagnosi della malattia del dipendente?
Il datore di lavoro non è legittimato a raccogliere certificati di malattia dei dipendenti con l'indicazione della diagnosi. In assenza di specifiche deroghe previste da leggi o da regolamenti, il lavoratore assente per malattia deve fornire un certificato contenente esclusivamente la prognosi con la sola indicazione dell'inizio e della durata dell'infermità.

Quali informazioni devono essere contenute nei certificati medici che attestino l'idoneità al servizio?
Nei certificati medici legali che attestano l'idoneità al servizio di un lavoratore, deve essere riportato il solo giudizio medico legale senza diagnosi, anziché il verbale integrale della visita collegiale.

Il datore di lavoro può pubblicare informazioni sulla salute dei dipendenti?
Sia le imprese private, sia la Pubblica Amministrazione devono tutelare con la massima diligenza le informazioni sulla salute dei propri dipendenti, così come quella dei dirigenti, evitando che vengano divulgate. L'utilizzo ingiustificato di questi dati può creare disagio alla persona o esporla a conseguenze indesiderate.

5) TELECAMERE ED INTERNET

Possono essere installate delle telecamere in ospedali e luoghi di cura?

L'eventuale controllo di ambienti sanitari ed il monitoraggio di pazienti ricoverati in particolari locali (ad es. nelle unità di rianimazione o in reparti di isolamento) devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cure e tutela della salute degli interessati.

Chi può vedere le immagini riprese nei luoghi di cura?
La visione delle immagini deve essere consentita solo al personale autorizzato (ad es. medici ed infermieri) ed ai familiari dei ricoverati. Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video di ricoverati in reparti dove non sia consentito a parenti ed amici di recarsi personalmente (ad es. in rianimazione): a questi ultimi può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente. Non bisogna quindi collocare i monitors in locali liberamente accessibili al pubblico. La diffusione di immagini idonee a rivelare lo stato di salute è infatti vietata.

Il paziente può ottenere la copia della registrazione video del proprio intervento?
L'interessato ha diritto di accedere a tutti i dati personali che lo riguardano, in qualunque documento, supporto anche visivo o archivio in cui esse siano contenute, senza dover fornire giustificazioni della necessità di ottenere tali informazioni. Può così accedere anche alle fotografie scattate prima e dopo gli interventi chirurgici e chiederne copia, così come può ottenere il video dell'operazione e ogni altra informazione che lo riguardi.

L'elenco dei degenti di un ospedale può essere pubblicato sul web?
E' vietata la diffusione di dati idonei a rivelare lo stato di salute. Non possono quindi essere resi disponibili a chiunque su internet i dati anagrafici, l'indicazione delle diagnosi o i risultati delle analisi cliniche delle persone che si recano presso un ospedale.

L'elenco dei degenti di un ospedale può essere pubblicato sul web?
E' vietata la diffusione di dati idonei a rivelare lo stato di salute. Non possono essere quindi resi disponibili a chiunque su internet i dati anagrafici, l'indicazione delle diagnosi o i risultati delle analisi cliniche delle persone che si recano presso un ospedale.

E' possibile caricare foto o altre informazioni relative a degenti sulla propria pagina di facebook o di altri social network?
Attenzione a non pubblicare dati personali, ad esempio nomi o fotografie, di pazienti sulle proprie pagine di social network. Anche se spesso si pensa di condividerle solo con amici, magari colleghi sanitari, si rischia invece di diffonderle ad un numero imprecisato di utenti sulla rete, violando così la privacy delle persone coinvolte.

6) SANITA' ELETTRONICA

Il paziente è obbligato ad adottare il fascicolo sanitario elettronico?
NO. Il paziente deve poter scegliere, in piena libertà, se far costituire o meno un fascicolo sanitario elettronico (Fse) con tutte o solo alcune delle informazioni sanitarie che lo riguardano. Deve quindi ricevere un'adeguata informativa che chiarisca chi (medici di base, del reparto ove è ricoverato, farmacisti……) ha accesso ai suoi dati e come possono essere utilizzati. Deve poter manifestare un consenso autonomo e specifico, distinto da

quello che si presta ai fini di cura della salute. Al paziente deve, inoltre, essere garantita la possibilità di "oscurare" la visibilità di alcuni eventi clinici. Se il paziente non vuole aderire al Fse deve comunque poter usufruire delle prestazioni del Servizio Sanitario Nazionale.

Chi può accedere al fascicolo sanitario elettronico?
Il fascicolo può essere consultato dal paziente con modalità adeguate (ad es. tramite smart card) e dal personale sanitario strettamente autorizzato per finalità sanitarie (prevenzione, diagnosi, cura e riabilitazione dell'interessato). Non potranno accedervi invece periti, compagnie di assicurazione, datori di lavoro.

I referti medici possono essere inviati all'assistito tramite internet?
SI. I risultati di analisi cliniche, radiografie e referti medici possono essere inviati direttamente sulla e-mail del paziente o possono essere resi consultabili on line dal computer di casa. L'adesione al servizio dovrà però essere facoltativa ed il referto cartaceo rimarrà comunque disponibile. L'assistito dovrà dare il suo consenso sulla base di una informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di consultazione o consegna on line dei referti. Le strutture che offrono la possibilità di archiviare e continuare a consultare via web i referti dovranno fornire una ulteriore specifica informativa ed acquisire un autonomo consenso.

Quanto tempo potranno essere conservati on line i referti?
Il referto potrà rimanere consultabile on line solo per un periodo di tempo limitato di quarantacinque (45) giorni. Dovrà, inoltre, essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta del paziente.

7) HIV

Il medico può chiedere al suo paziente se è sieropositivo?
Coloro che esercitano la professione sanitaria non possono raccogliere, al momento dell'accettazione, informazioni sulla sieropositività del paziente, a meno che ciò non risulti indispensabile per il tipo di intervento o terapia che si deve seguire. In ogni caso, il dato dell'infezione da Hiv (virus dell'immunodeficienza) deve essere raccolto direttamente dal medico, non dal personale amministrativo e sempre con il consenso del paziente.

In questo caso, come si concilia la tutela della privacy con la sicurezza del personale medico?
La normativa di settore prevede che siano adottate specifiche misure di protezione dal contagio nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività. L'esigenza di ottenere informazioni sull'infezione da Hiv fin dal momento dell'accettazione non può dunque essere giustificata dalla necessità di attivare tali misure. Nel caso in cui il medico venga a conoscenza di un caso di Aids o di Hiv, oltre a rispettare specifici obblighi di segretezza e non discriminazione nei confronti del paziente, ha l'obbligo di adottare ogni misura individuata dal Codice della privacy per garantire la sicurezza dei dati sanitari.