ALLEGATO "C" A DELIBERA N. 207 DEL 01 SET. 2015

1. CAMPO DI APPLICAZIONE

Il presente documento si rivolge a tutti i soggetti, dipendenti e non, compresi i soggetti con incarico libero professionale o altro personale non strutturato, che effettuano, anche a titolo volontario (ove non incaricati all'uopo dalla Associazione di appartenenza che intrattenga specifici rapporti convenzionali con ISPO), operazioni di trattamento dei dati personali per conto di ISPO.

2. NORMATIVE DI SETTORE

Restano in vigore alcune normative di settore (es. osservanza segreto professionale, tutela della dignità del paziente, soprattutto con riguardo a fasce deboli (disabili, minori, anziani), la riservatezza nei colloqui e delle informazioni sulla salute, sulle prescrizioni mediche e sulle cartelle cliniche), che si affiancano al Codice della Privacy, nel loro ambito specifico, nella definizione dei requisiti di legittimazione dei relativi trattamenti.

3. TRATTAMENTO DI DATI PERSONALI

Qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Si ha trattamento di dati anche quando le suddette operazioni:
- siano effettuate senza l'ausilio di strumenti elettronici,
- riguardino dati non registrati in banche di dati (ovvero dati conservati in archivi non organizzati).

Dal punto di vista strutturale, il trattamento dei dati è sostanzialmente un processo, caratterizzato dalle seguenti operazioni:
- una fase di input, ovvero di raccolta e registrazione dei dati, tramite loro acquisizione dall'interessato o presso terzi;
- una fase di operazioni interne: organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, cancellazione e distruzione di dati;
- una eventuale fase di output, ovvero di comunicazione o diffusione dei dati stessi.

Dalla definizione normativa di trattamento sopra richiamata si inferisce che il trattamento dei dati inizia fin dalla fase della raccolta delle informazioni e non riguarda la sola fase di elaborazione e comunicazione/diffusione; da cui l'obbligo ad es. che l'informativa che deve normalmente essere preventiva, sia appunto data prima della raccolta stessa dei dati.

Il trattamento di dati personali è ammesso solo da parte del titolare, dei responsabili e degli incaricati; l'Istituto non consente il trattamento di dati da parte di personale non individuato e legittimato, a pena di incorrere in un trattamento illegittimo passibile di sanzioni.

Il Codice, all'art. 11, stabilisce che i dati personali devono essere:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

In sintesi, per soddisfare il principio di liceità il trattamento dei dati deve rispettare:
- presupposti e limiti stabiliti dal Codice, dalle leggi, dai regolamenti e dalle disposizioni dell'Autorità Garante;
- eventuali disposizioni contenute nei codici di deontologia e di buona condotta di cui all'allegato A del Codice, promossi dal Garante per determinati settori;
- misure minime di sicurezza di cui agli artt. 31-36 del Codice;
- normative di settore (es. osservanza segreto professionale, tutela della dignità del paziente, soprattutto con riguardo a fasce deboli (disabili, minori, anziani), la riservatezza nei colloqui e delle informazioni sulla salute, sulle prescrizioni mediche e sulle cartelle cliniche).

I dati sono trattati correttamente se il trattamento è svolto con la consapevolezza dell'interessato; da ciò consegue l'obbligo di una informativa che sia idonea (attraverso l'utilizzo di una terminologia comprensibile e al tempo

stesso esaustiva) a rendere l'interessato convenientemente edotto dei trattamenti dei dati che lo riguardano (l'inidoneità o addirittura l'omissione dell'informativa sono specificamente sanzionate).
Per ogni trattamento occorre una finalità determinata (cioè stabilita a priori), presente ed attuale (cioè tuttora valida), esplicita (cioè resa conoscibile) e lecita, la quale costituisce il parametro di riferimento per valutare i dati da trattare, sia in termini qualitativi che quantitativi. Le operazioni di trattamento non devono essere incompatibili con tali finalità (c.d. principio di finalità).
Per gli enti pubblici tali finalità devono essere utili a soddisfare i rispettivi scopi istituzionali, nel senso che un ente pubblico non può effettuare trattamenti che non rientrino tra le proprie finalità istituzionali. In particolare, per assicurare maggiori garanzie agli interessati, i trattamenti di dati sensibili e giudiziari effettuati da un ente pubblico sono leciti solo se riferibili a finalità di rilevante interesse pubblico individuate dalla legge. Quando la finalità è raggiunta o diviene irraggiungibile è necessario provvedere alla cancellazione o alla trasformazione in forma anonima dei dati, fatte salve le disposizioni in materia di archiviazione e conservazione dei documenti amministrativi. Ciò consente, tra l'altro, di prevenire possibili accessi abusivi ad informazioni non più attuali. E' considerato compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati l'ulteriore trattamento per fini storici, di ricerca scientifica o di statistica.
Il principio di pertinenza e non eccedenza sancisce l'obbligo di assicurare la proporzionalità tra mezzi impiegati e fini perseguiti, raccogliendo solo i dati strettamente funzionali e necessari per il raggiungimento degli scopi legittimi perseguiti, completi e non eccessivi rispetto agli scopi stessi. Per il cd. principio di necessità, invece, devono essere applicate ai dati modalità di trattamento che permettano appunto di identificare l'interessato solo in caso di necessità. Il Codice prescrive dunque all'art. 3 di:
- ridurre al minimo l'utilizzazione di dati personali ed identificativi;
- non utilizzare dati personali se è possibile utilizzare dati anonimi;
- se occorre utilizzare dati personali, utilizzare dati personali identificativi solo quando necessario.

In accordo a tale principio i sistemi informativi debbono essere predisposti e configurati per ridurre al minimo l'uso di dati personali ed identificativi, specie quando le finalità di trattamento possono essere raggiunte utilizzando dati anonimi. In particolare, qualora il dato sia trattato da un soggetto pubblico, la norma richiede che siano trattati i soli dati essenziali per lo svolgimento delle attività istituzionali e che siano svolte le sole operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.

4. TRATTAMENTO DI DATI SENSIBILI

Ai sensi dell'art. 22 comma 6 del *Codice*, i dati sensibili contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici, devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
I dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

5. INTERESSATO

Informativa

L'interessato deve ricevere, antecedentemente o al momento della raccolta dei dati, una idonea informativa. L'informativa è la dichiarazione che il titolare o il responsabile del trattamento fornisce all'interessato relativamente all'utilizzo che intende fare delle informazioni che lo riguardano ed ai suoi diritti. Essa indica:
- le finalità per le quali e le modalità con le quali verranno trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati da parte dell'interessato;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o trasmessi e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo all'art. 7 del Codice;
- il nominativo del Titolare e del Responsabile (o dei Responsabili).

In ambito sanitario l'informativa è resa di norma per iscritto, se necessario integrandola oralmente, anche in riferimento ad una pluralità di prestazioni ed anche tramite affissione di appositi manifesti nei locali di accesso all'utenza.
Non è, dunque, necessario dare un'informativa per ogni accesso dell'interessato, nel senso che gli organismi sanitari pubblici possono fornire un'informativa per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, in riferimento ad una pluralità di prestazioni erogate anche da distinte unità dello stesso organismo.
Nel caso di trattamento di dati genetici l'informativa deve inoltre evidenziare:

- l'esplicitazione analitica di tutte le specifiche finalità perseguite;
- i risultati conseguibili, anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;
- il diritto dell'interessato di opporsi al trattamento dei dati genetici per motivi legittimi;
- la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale l'utilizzo di questi per ulteriori scopi;
- il periodo di conservazione dei dati genetici e dei campioni biologici.

Diritto di accesso ai dati
Ai sensi dell'art. 7 del Codice, l'interessato ha diritto di:
- conoscere, mediante accesso gratuito, l'esistenza di trattamenti di dati che possono riguardarlo;
- essere informato su:
  - il nome e il domicilio del Titolare e del Responsabile del trattamento;
  - le finalità e le modalità del trattamento;
  - l'eventuale ambito di comunicazione e diffusione;
- ottenere a cura del titolare o del responsabile, senza ritardo:
  - la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento.

L'interessato ha inoltre il diritto a:
- ottenere a cura del titolare o del responsabile, senza ritardo:
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'aggiornamento, la rettifica ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- l'attestazione che le operazioni di cui sopra sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
- opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Tutte le istanze di accesso ex art. 7 del Codice sono comunicate al Referente aziendale per la privacy, che predispone il riscontro all'interessato; se la richiesta è relativa a dati sanitari, la comunicazione deve essere sottoscritta da parte di un medico.

Consenso
Per i trattamenti di dati direttamente connessi alla erogazione di prestazioni sanitarie, i pazienti devono esprimere il proprio consenso al trattamento.
Il consenso, secondo i principi generali richiamati dall'art. 23 del Codice è validamente prestato dall'interessato (o da altro soggetto legittimato) solo:
- se è espresso liberamente;
- se è espresso specificamente in riferimento ad un trattamento chiaramente individuato;
- se è stata data idonea informativa all'interessato.

Relativamente alla prestazione del consenso, laddove necessaria, è opportuno precisare che:

- non è necessario ottenere un consenso per ogni accesso dell'interessato, ovvero il consenso può essere prestato con modalità semplificate: può cioè essere manifestato con un'unica dichiarazione e, per gli organismi sanitari pubblici, anche in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti;
- non è necessario che il consenso sia prestato in forma scritta; il consenso può dunque essere prestato anche oralmente. In tal caso deve perciò essere documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico;
- il consenso può essere prestato, in particolari casi, anche successivamente alla prestazione, in caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente.

Può altresì essere prestato senza ritardo, successivamente alla prestazione, anche in caso di:

- impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato;
- rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato;
- prestazione medica che può comunque essere pregiudicata dalla preventiva comunicazione dell'informativa, in termini di tempestività o efficacia (es. ferito su un'ambulanza, di cui non si conoscono le reali condizioni).

Misure per il rispetto dei diritti dell'interessato

Non risulta mai giustificata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare. Non devono essere, parimenti, resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'interessato.

Nell'informativa fornita all'interessato occorre specificare che, in occasione di alcune prestazioni sanitarie, si perseguono anche finalità didattiche, oltre che di cura e prevenzione. Durante tali prestazioni devono comunque essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e *rispettando eventuali legittime volontà contrarie.*

Comunicazione all'interessato di dati idonei a rivelare lo stato di salute

L'art. 84 del *Codice*, inserito nel Titolo V *Trattamento di dati in ambito sanitario*, è rubricato *Comunicazione di dati all'interessato*; per quanto riguarda il soggetto che può effettuare tale comunicazione, questi è in primo luogo il medico. Per l'art. 84 c. 1 del *Codice* infatti:

> I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato (...) da parte di esercenti le professioni sanitarie ed organismi sanitari, *solo per il tramite di un medico designato dall'interessato o dal titolare.*

La comunicazione all'interessato (o ad altro soggetto autorizzato) di tali dati da parte di un esercente la professione sanitaria *diverso dal medico* è, in quanto tale, carente di legittimazione. Quest'ultima può però essere sanata: il titolare (ovvero l'Istituto) o il responsabile possano autorizzare *per iscritto* esercenti le professioni sanitarie *diversi dai medici*, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute. L'"atto di incarico" deve individuare "appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati".

Nell'assenza di questo presupposto - autorizzazione scritta da parte del titolare o responsabile - una comunicazione effettuata direttamente al paziente o al soggetto autorizzato da un esercente la professione sanitaria non medico non appare legittima.

L'art. 84 non si applica alle informazioni direttamente date dall'interessato (es. restituzione di documentazione sanitaria precedentemente consegnata dall'interessato).

6. RESPONSABILI DEL TRATTAMENTO

Si tratta di soggetti, individuati dal Titolare, che hanno il compito di collaborare per l'applicazione, nelle realtà operative di rispettiva competenza, delle idonee misure per assicurare il diritto alla protezione dei dati personali.
La loro individuazione, facoltativa per l'art. 29 del Codice, è stata prevista come obbligatoria, per gli enti sanitari, da Regione Toscana (cfr. Delibera G.R.T. del 29 novembre 2004 Linee guida alle Aziende sanitarie per l'applicazione del D.Lgs. 196/2003).
L'Istituto individua quali responsabili del trattamento:
- il **Direttore Amministrativo** e il **Direttore Sanitario**, ciascuno per il settore di rispettiva competenza e per tutte quelle operazioni facenti espressamente capo alla Direzione Aziendale;
- i **Direttori di strutture organizzative complesse e delle strutture semplici afferenti alla Direzione Aziendale** o, in vacanza di incarico, secondo quanto previsto, in tema di sostituzioni, dal vigente Regolamento di Organizzazione e Funzionamento dell'Istituto;
- i **Responsabili dei Coordinamenti assistenziale, tecnico-sanitario e statistico delle aree del Comparto** o, in vacanza di incarico, i coordinatori facenti funzione individuati dalla Direzione Aziendale.

Possono inoltre essere individuati dal Titolare, quali responsabili, altri dirigenti o funzionari, in virtù delle particolarità organizzative e funzionali delle attività di competenza.
Nell'ambito di un progetto di sperimentazione, lo sperimentatore principale (P.I.) è individuato quale responsabile del trattamento.
Il responsabile del trattamento ha il compito di individuare, in relazione ai trattamenti di dati personali effettuati nelle strutture afferenti alla propria area di competenza ed in collaborazione con il Referente aziendale per la privacy, adeguate misure organizzative e gestionali dirette ad assicurare a tutti i soggetti interessati il diritto alla riservatezza ed alla protezione dei dati personali e dunque ad evitare trattamenti dei dati non consentiti nonché ad assicurare una puntuale gestione degli archivi cartacei ed una corretta archiviazione dei dati trattati con strumenti informatici.
Più in particolare, relativamente ai trattamenti di dati personali effettuati nelle strutture afferenti alla propria area di competenza, il responsabile del trattamento, anche avvalendosi, ove occorra, della collaborazione del Referente aziendale per la privacy, deve:
- vigilare sull'osservanza delle istruzioni impartite dal Titolare (in particolare con il presente documento);
- identificare, censire e periodicamente verificare i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza. I Responsabili del trattamento periodicamente devono comunicare al Referente aziendale per la privacy e aggiornare, in caso di modifica, attivazione o cessazione, l'elenco dei trattamenti effettuati nell'ambito della propria struttura e le relative misure di sicurezza adottate.
- definire per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o anomizzazione dei dati obsoleti, nel rispetto della normativa in materia di tenuta archivi;
- far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti, in particolare, comunicare preventivamente al Titolare, per il tramite del Referente aziendale per la privacy, l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare, per il tramite del Referente aziendale per la privacy, l'eventuale cessazione del trattamento (art. 16 codice);
- verificare che all'interessato o al soggetto presso il quale sono raccolti i dati personali sia data l'informativa di cui all'art. 13 del Codice, se necessario coordinandosi con il Referente aziendale per la privacy per la sua redazione e modalità di comunicazione;
- verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;
- individuare tra i propri collaboratori gli Incaricati del trattamento, nominandoli con atto scritto che deve contenere anche le istruzioni cui devono attenersi nell'ambito del trattamento consentito – integrative di quelle fornite dal Titolare, precisando compiti e mansioni;
- stabilire idonei profili di autorizzazione dei propri incaricati agli applicativi informatici, nel rispetto dei principi di necessità, pertinenza e non eccedenza;

- assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali (art. 19 codice Privacy);
- attenersi, per i dati relativi ad attività di studio e di ricerca (art. 100 codice Privacy), alla disciplina secondo la quale è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
- formulare adeguate proposte alla Direzione Aziendale, quando le soluzioni individuate non possano essere adottate facendo ricorso a misure organizzative interne alla struttura di pertinenza;
- adempiere agli obblighi di sicurezza, quali:
    - adottare le misure minime di sicurezza espressamente previste dal Codice (vedi allegato n. 3 al presente documento).
    - adottare tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione e perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 codice Privacy);
    - comunicare tempestivamente al Titolare casi di accesso non autorizzato ai dati o di trattamento non consentito o non conforme alle finalità istituzionali.

La funzione di Responsabile del trattamento dei dati, per il suo carattere fiduciario, è attribuita personalmente e non è suscettibile di delega.
I responsabili possono designare dei sostituti in caso di loro assenza o impedimento.
Il Responsabile del trattamento si avvale dei propri collaboratori per stabilire continuativi rapporti di informazione e coordinamento con il Referente aziendale per la privacy.
Il Responsabile del trattamento è formalmente delegato ad individuare, per i trattamenti di competenza, e con il supporto del Referente aziendale per la privacy, i soggetti esterni legittimati a trattare i dati personali di cui l'Azienda è Titolare.
Ogni modifica di responsabilità delle strutture organizzative afferenti al Responsabile del Trattamento deve essere segnalata al Referente aziendale per la privacy.

7. INCARICATI DEL TRATTAMENTO

Gli incaricati sono, ai sensi dell'art. 30 del Codice, le persone fisiche autorizzate a compiere operazioni di trattamento dal responsabile o dal titolare.
Sono coloro che materialmente effettuano, attenendosi alle istruzioni impartite dal titolare e dal responsabile, le operazioni di trattamento di dati: nel contesto aziendale, dunque, con modalità ed abilitazioni diverse secondo le rispettive competenze, trattasi tanto di personale sanitario che tecnico o amministrativo.
La designazione degli incaricati deve essere effettuata dal Responsabile del Trattamento per iscritto ed individuare puntualmente l'ambito del trattamento consentito (si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale sia individuato, per iscritto, l'ambito del trattamento consentito ai suoi addetti). La designazione deve essere aggiornata in relazione al trasferimento presso altra struttura dell'Istituto o alla modifica delle attribuzioni/competenze che modifichino i trattamenti dei dati personali per i quali è autorizzato l'incarico.
I responsabili del trattamento dovranno, a loro volta, qualora ritenuto opportuno o necessario, predisporre indicazioni scritte agli incaricati di propria pertinenza – distinti per categorie – integrative di quelle fornite dal Titolare sull'ambito di trattamento consentito, precisando compiti e mansioni.
L'ambito dei trattamenti consentiti ai singoli incaricati e gestiti con supporti informatici e/o cartacei, necessari all'espletamento delle attività istituzionali, deve esser verificato ed aggiornato periodicamente dal Responsabile del Trattamento, con cadenza almeno annuale.
Gli incaricati possono aver accesso esclusivamente ai dati personali la cui conoscenza sia strettamente necessaria o indispensabile per l'espletamento delle attività cui sono preposti.
Le designazioni sono estese, con analoghi criteri e modalità, anche ai non dipendenti, e più in particolare a quei soggetti che funzionalmente svolgono operazioni di trattamento su dati di cui l'Istituto ha la titolarità, quali i soggetti con incarico libero professionale o altro personale non strutturato. Ciò vale ovviamente anche, ove non previsto da specifiche Convenzioni di ISPO con strutture pubbliche o private, per dottorandi di ricerca, borsisti, nonché volontari, tirocinanti o laureandi che accedano ai pazienti per acquisire informazioni necessarie per la tesi

(si sottolinea che la somministrazione di un questionario prevede anche la comunicazione agli interessati di una idonea informativa sul trattamento dei dati).

8. REFERENTE AZIENDALE PER LA PRIVACY

Il Referente aziendale per la privacy svolge i seguenti compiti:
- garantisce il supporto alla Direzione Aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia, segnatamente in tema di notificazione al Garante ex art. 37 del Codice e comunicazioni al Garante ex artt. 39 e 41 del Codice;
- vigila sull'osservanza delle istruzioni contenute nel presente documento;
- tiene ed aggiorna un censimento dei trattamenti effettuati in Istituto sulla base delle comunicazioni effettuate dai responsabili del trattamento;
- tiene e aggiorna l'elenco dei responsabili del trattamento in ambito aziendale;
- tiene ed aggiorna l'elenco degli archivi cartacei e/o magnetici contenenti dati personali custoditi a livello aziendale, sulla base delle informazioni inviategli dai responsabili delle strutture competenti;
- propone, svolge e/o coordina l'attività di formazione in tema di normativa sulla riservatezza dei dati, assicurando la promozione della cultura della privacy a livello aziendale;
- gestisce i riscontri alle istanze degli interessati ex art. 7 del Codice, e si attiva per comporre le controversie sui dati personali;
- fornisce la necessaria consulenza in ordine alle problematiche in tema di riservatezza, in particolare collaborando con i responsabili del trattamento;
- propone l'adeguamento dei percorsi e delle procedure aziendali per quanto attiene l'aspetto della riservatezza dei dati;
- si occupa dei conflitti tra diritto alla riservatezza dei dati e dovere di garantire la trasparenza dell'attività amministrativa.

9. OBBLIGHI DI NOTIFICAZIONE AL GARANTE

La procedura di notificazione è seguita dal Referente aziendale per la privacy. E' fatto obbligo a ciascun responsabile del trattamento di fornire al Referente aziendale per la privacy tutti gli elementi informativi necessari per effettuare la notificazione di cui sopra, quale presupposto di legittimità del trattamento che si intende attivare.

10. OBBLIGHI DI COMUNICAZIONE AL GARANTE

E' fatto obbligo a ciascun responsabile del trattamento di fornire al Referente aziendale per la privacy tutti gli elementi informativi necessari per effettuare la comunicazione di cui sopra, quale presupposto di legittimità del trattamento che si intende attivare. I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione, salvo diversa determinazione anche successiva del Garante.

11. DOCUMENTAZIONE SANITARIA INFORMATIZZATA

L'Autorità Garante il 16 luglio 2009 ha adottato un provvedimento recante *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario.* Il Garante, con i termini *fascicolo sanitario* e *dossier sanitario elettronico* si riferisce al trattamento, attraverso strumenti informatici, di insiemi di dati e documenti sanitari (es.: referti) riferiti logicamente ad un medesimo soggetto, allo scopo di documentarne la storia clinica.
Una cartella clinica elettronica, o scheda ambulatoriale per ISPO, ha una finalità primaria di tutela della salute, ovvero di prevenzione, diagnosi, cura e riabilitazione, dell'interessato, ma può avere anche una finalità in senso lato medico-legale; non è escluso infatti, pur attivandosi secondo modalità peculiari, un suo utilizzo per scopi di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria o di ricerca scientifica, epidemiologica o statistica.

12. COMUNICAZIONI AL MEDICO DI FAMIGLIA

In ambito sanitario, deve ritenersi coperta da segreto professionale ogni notizia riguardante la vita privata dell'assistito che quest'ultimo non abbia interesse a rivelare e della quale il medico sia venuto a conoscenza in quanto medico.

Consideriamo i seguenti possibili casi di trasmissione del segreto detenuto da un medico dell'Istituto:

- ad altro medico della medesima Istituto;
- ad altro medico di diverso Istituto;
- al medico di famiglia.

Si fa presente che nel primo caso ci si muove nel medesimo ambito di titolarità, per cui si ha propriamente una *trasmissione* di dati idonei a rivelare lo stato di salute; negli altri casi, trattandosi di comunicazioni tra diversi titolari del trattamento (il medico di famiglia è anzi un soggetto privato autonomo titolare del trattamento), si ha una *comunicazione* di dati idonei a rivelare lo stato di salute.

Nel primo caso è sufficiente che la messa a disposizione dei dati sia fatta, nel rispetto del principio di necessità/indispensabilità, ad altro soggetto incaricato del trattamento; si richiede in particolare, ai sensi dell'art. 85 comma 4 del *Codice*, che l'utilizzazione delle diverse tipologie di dati sia consentita "ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività (...) secondo il *principio dell'indispensabilità* dei dati di volta in volta trattati".

Nel secondo caso è necessario lo specifico consenso dell'interessato.

Nel terzo caso, stante l'improbabilità di poter legittimamente individuare il Medico di medicina generale come responsabile esterno del trattamento, è necessario lo specifico consenso dell'interessato.

13. COMUNICAZIONI TELEFONICHE CON GLI ASSISTITI

E' necessaria una comunicazione la più laconica possibile: nel caso occorra comunicare la data di una prestazione (anche nel senso del suo spostamento) è sufficiente richiamare ad es. la data precedentemente comunicata e la nuova, senza specificare la prestazione o il reparto.

Dunque, qualora sia necessario contattare il paziente telefonicamente, è necessario fornirgli una informativa preventiva in cui lo si invita a rilasciare un recapito telefonico al quale l'Istituto possa, qualora necessario e salva contraria volontà dell'assistito, effettuare eventuali comunicazioni la cui tipologia sarà convenientemente specificata; l'informativa deve essere redatta in modo che faccia anche chiaramente intendere che la comunicazione avverrà al recapito, e solo per quanto possibile - non necessariamente, in quanto impossibile da accertare - al soggetto interessato.

E' ovviamente preferibile poter effettuare tali comunicazioni ad un telefono cellulare, presumibilmente nell'esclusiva disponibilità dell'interessato.

Occorre comunque porre in atto soluzioni organizzative che rendano eccezionali tali comunicazioni, rimuovendo tutte quelle procedure che prevedano la comunicazione telefonica come inevitabile (es. preventiva raccolta delle richieste d'esame e successiva definizione dell'agenda appuntamenti).

Qualora venga richiesto telefonicamente se un referto è pronto o meno, pur ottenute indicazioni sufficienti sulla legittimazione del richiedente, è comunque necessario limitare la risposta ad un assenso o ad una negazione; l'amministrativo incaricato del trattamento non può mai comunicare eventuali valori riportati nel referto.

Qualora si ritenga opportuno comunicare risultati via telefono, è necessario che:

- la comunicazione sia effettuata da un medico o da altro esercente la professione sanitaria specificamente autorizzato dal Titolare o dal Responsabile;
- sia utilizzato un identificativo del paziente, diverso volta a volta per le successive prestazioni, che questo debba comunicare telefonicamente per poter aver accesso alla comunicazione dei dati.

14. DEFINIZIONI

Dati personali: qualunque informazione relativa ad un soggetto - persona fisica, persona giuridica, ente od associazione - identificato o identificabile (anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale).

Dati anonimi: i dati che, in origine o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile.
Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dati idonei a rivelare lo stato di salute: informazioni tali da svelare, anche indirettamente uno stato patologico o comunque almeno uno stato di normalità compromessa.
Dati giudiziari: i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.
Dati genetici: i dati che, indipendentemente dalla tipologia, identificano le caratteristiche del patrimonio genetico di un individuo trasmissibili nell'ambito di un gruppo di persone legate da vincoli di parentela.
Trattamento: qualunque operazione o complesso di operazioni effettuato sui dati personali (raccolta, registrazione, organizzazione, conservazione; consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco comunicazione, diffusione, cancellazione, distruzione di dati). Rientrano nella nozione di trattamento anche le operazioni effettuate senza l'ausilio di strumenti elettronici, nonché quelle relative ad informazioni non organizzate in banche dati. **Comunicazione**: il dare conoscenza dei dati personali a uno o più soggetti determinati (diversi dall'interessato, dal responsabile e dagli incaricati), in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Trasferimento: ogni spostamento anche temporaneo di informazioni, tanto all'interno che all'esterno dell'ambito di titolarità del trattamento.
Titolare: il soggetto - persona fisica, persona giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo - cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso.
Responsabile: il soggetto - persona fisica, persona giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo - preposto dal Titolare al trattamento di dati personali.
Incaricato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal responsabile, in pratica chi materialmente effettua le operazioni di trattamento di dati.
Interessato: il soggetto (persona fisica, persona giuridica, ente o associazione) cui si riferiscono i dati personali.
Amministratore di sistema: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Garante per la Protezione dei dati personali: organo collegiale che ha, tra l'altro, il compito di:
- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati;
- prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
- vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco;
- promuovere la sottoscrizione di codici deontologici;
- esprimere pareri nei casi previsti.

Gruppo di lavoro ex articolo 29 direttiva 95/46/CE: istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle Autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.