BURLO

Direzione Amministrativa
S.C. Affari Generali e Legali
CERTIFICATO CISQ/CERTIQUALITY n. 7889- IQNet n. 38050
Fax. 040 762623 *e mail*: ufficio.legale@burlo.trieste.it
Posta certificata:oiburlotsprotgen@certsanita.fvg.it

Prot. n. 12789/A del 14 DIC. 2012

POLITICA PRIVACY

REQUISITI NORMA ISO 9001:2008 P.TO 4.2
STANDARD JCI QPS.2

ATTRIBUZIONE DEL DOCUMENTO

DESTINATARIO
S.C. AFFARI GENERALI E LEGALI
RESPONSABILE SISTEMA QUALITÀ AZIENDALE
DIREZIONE GENERALE
DIREZIONE AMMINISTRATIVA
DIREZIONE SANITARIA
S.C. SERVIZIO ECONOMICO FINANZIARIO
S.C. INGEGNERIA CLINICA, ACQUISIZIONE TECNOLOGIE, BENI E SERVIZI

REDAZIONE	APPROVAZIONE	
S.C. AFFARI GENERALI E LEGALI	**DIRETTORE GENERALE**	**DIRETTORE AMMINISTRATIVO**
AVV. BENEDETTA SMEDILE	PROF. MAURO MELATO	DOTT. STEFANO DORBOLÒ
	DIRETTORE SANITARIO	**DIRETTORE SCIENTIFICO**
	DOTT. DINO FARAGUNA	PROF. GIORGIO ZAULI
	AREA QUALITÀ	
	DOTT. SSA PATRIZIA VISCONTI	

POLITICA PRIVACY

INDICE

1. SCOPO

Scopo della seguente politica è quello di definire le modalità inerenti l'applicazione della normativa sulla privacy per le tutte Strutture del'IRCCS Burlo Garofolo, di seguito denominato per brevità "Istituto", al fine di garantire:
a) la protezione da perdita, distruzione, manomissione, accesso o uso non autorizzato dei dati sensibili contenuti nelle cartelle cliniche e in quelle ambulatoriali e di tutte le altre informazioni riguardanti i pazienti che accedono alle strutture aziendali;
b) l'accesso alle informazioni sanitarie solo a personale autorizzato, corrispondente alle proprie esigenze e alle responsabilità delle proprie mansioni.

2. CAMPO DI APPLICAZIONE

La politica sulla privacy si applica a tutto il personale dell'Istituto che è il *Titolare del trattamento* come entità nel suo complesso, rappresentato dal Direttore Generale *pro tempore*.

Tutti gli operatori dell'Istituto si impegnano a rispettare, nell'espletamento delle proprie attività, le modalità di protezione da perdita, distruzione, manomissione, accesso o uso non autorizzato dei dati sensibili contenuti nelle cartelle cliniche e in quelle ambulatoriali e di tutte le altre informazioni riguardanti i pazienti che accedono alle strutture aziendali nel rispetto delle vigenti disposizioni in materia di *privacy*.

I dipendenti dell'Istituto nonché tutte le persone che prestano attività all'interno dell'Istituto stesso a qualsiasi titolo, con o senza retribuzione compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dall'Istituto sono tenuti:

a) ad attenersi alla massima riservatezza rispetto alle notizie ed alle informazioni di cui vengono a conoscenza;

b) ad astenersi da operazioni attinenti al trattamento dei dati personali, qualora non siano individuati quali incaricati.

Il Responsabile del trattamento fornisce le necessarie informazioni alle persone che operano a qualsiasi titolo nella propria struttura.

I responsabili del trattamento dei dati, in relazione alla loro specifica funzione e sede, sono riportati in un apposito elenco presso l'Ufficio per le Relazioni con il Pubblico dell'Istituto; l'elenco è anche riportato nel sito Intranet alla Voce *Privacy: elenco Responsabili del trattamento dei dati.*

3. TERMINOLOGIA

Ai fini della presente procedura, si applicano le definizioni riportate nel "Codice in materia di protezione dei dati personali" (c.d. Codice della privacy), approvato con D.Lgs. 30.06.2003 n.196 ed in particolare:.

Banca Dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti. L'Azienda, nell'esercizio delle sue funzioni istituzionali, utilizza 1) Banche dati di tipo cartaceo; 2) Banche dati di tipo elettronico, utilizzabili con l'impiego di computer: a) collegati in rete locale; b) non collegati in rete locale; c) con collegamento ad internet.
Blocco	La conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Credenziale di autenticazione	Nel caso di utilizzo di sistemi informatici per il trattamento di dati personali, consiste in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo (utente + password) oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave. La parola chiave (password), quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Dato anonimo	Il dato che in origine, o a seguito di trattamento, non può essere associato in alcun modo ad un interessato identificato o identificabile.
Dati giudiziari	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, 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 ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4 comma 1 lettera e). Idonei quindi a rivelare comportamenti illeciti o fraudolenti, provvedimenti o procedimenti giudiziari, sanzionatori, disciplinari, amministrativi o contabili.
Dati identificativi	I dati personali che permettono l'identificazione diretta dell'interessato (art. 4 comma 1 lettera c). Alcuni esempi: nome, cognome, data e luogo di nascita, indirizzo, recapiti telefonici, codice fiscale, tipologia di esenzione sanitarie e fiscale.
Dato personale	Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4 comma 1 lettera b).
Dato personale pubblico	Dato personale di dominio pubblico (es. rubriche telefoniche pubbliche).
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 (art. 4 comma 1 lettera d). Alcuni esempi: i dati riferiti ai giorni di malattia dei dipendenti, la dichiarazione del versamento dell'8x1000 nella dichiarazione dei redditi, i certificati medici. Dati genetici: idonei a rivelare patologie rare e/o genetiche, malattie ereditarie, malformazioni congenite, trapianti di tessuti od organi o l'impiego di cellule staminali, ad accertare maternità o paternità nonchè relativamente alla procreazione.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Garante per la protezione dei dati personali	L'autorità di cui all'articolo 153 del D.Lgs. 196/2003, istituita con legge 31 dicembre 1996, n. 675.
Incaricati	Il Codice li definisce come le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (rif art. 4 comma1 lettera h e art. 30), specificando all'art.30 che "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite". Il Garante, dando fin dall'inizio un'interpretazione restrittiva, prevede che l'incaricato debba essere sempre ed esclusivamente una persona fisica, e mai una struttura organizzativa complessa. Verranno quindi considerati Incaricati, tutte le persone fisiche che

	fanno parte dell'organizzazione riferita all'attività del Titolare del Trattamento, sia che essi siano dipendenti, consulenti, agenti o in qualsiasi altra forma subordinata.
Interessato	La persona fisica, la persona giuridica,l'ente o l'associazione cui si riferiscono i dati personali (rif. art. 4 comma 1 lettera i).
Misure minime	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 31. Esse sono specificate nell'allegato B del codice. La loro omessa adozione è sanzionata penalmente ai sensi dell'art. 169 del codice.
Misure idonee	Esse non sono codificate, sono scelte e sviluppate dal Titolare in base alla valutazione del rischio. Devono essere adottate ai sensi dell'art. 31 del codice in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale di dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta. La mancata adozione o la inidoneità delle misure considerate non hanno rilevanza penale, ma possono determinare una responsabilità di natura risarcitoria ai sensi dell'art. 15 del codice. Quest'ultimo richiama l'art. 2050 del codice civile (riguardante le attività pericolose), per cui spetta al danneggiante/Azienda provare di aver adottato ogni misura idonea affinchè il danno non si verificasse.
Responsabile	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (rif. art. 4 comma 1 lettera g e art. 29). I confini generali di tale ruolo vengono delineati dal combinato disposto degli articoli 4 e 29 del codice, ai sensi dei quali si può definire responsabile: "il soggetto preposto dal titolare al trattamento dei dati personali, che deve essere individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza". Tale soggetto deve quindi possedere una competenza insieme tecnica e legale, in materia di privacy ed organizzativa.
Sistema di autorizzazione	Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Strumenti elettronici	Sono gli elaboratori, i programmi per elaboratori (ad esempio il software gestionale) e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (rif. art. 4 comma 3 lettera b). La definizione che il Codice della privacy attribuisce agli strumenti elettronici è molto chiara e va tenuta ben presente quando si va ad applicare le disposizioni del "Disciplinare Tecnico in materia di Misure Minime di Sicurezza" (Allegato B del Codice). E' quindi di fondamentale importanza, eseguire una scrupolosa analisi del proprio sistema informatico, assieme al proprio responsabile (o consulente esterno), per stabilire quali strumenti eseguono effettivamente i trattamenti di dati personali.
Titolare del trattamento	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza". Secondo l'art.28 è "l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza", ovvero l'Azienda stessa. Al titolare spetta quindi la direzione delle attività di trattamento dei dati personali e le decisioni strategiche di fondo su come (modalità) e perché (finalità) raccogliere e trattare i dati, nonché sull'organizzazione del trattamento e sulle risorse (strumenti) da dedicarvi, anche per garantire la sicurezza. Nel caso di strutture articolate in una struttura centrale e in una o più unità od organismi periferici dipendenti, il titolare è comunque l'azienda nel suo complesso. Se però l'unità o l'organismo periferico esercitano un potere decisionale del tutto autonomo, sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, il titolare diviene l'unità o l'organismo periferico stesso, per quanto riguarda i dati da esso trattati.
Trattamento	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dati, anche se non registrati in una banca di dati (art. 4 comma 1 lettera a).

4. INDIRIZZI GENERALI

Le modalità con le quali l'Istituto assicura la riservatezza dei dati delle persone assistite e la protezione/sicurezza dei dati stessi sono descritte nel Regolamento per la protezione dei dati personali, consultabile sul sito *Intranet* aziendale alla Voce *Privacy: Regolamento per la protezione dei dati personali.*

Gli utenti e assistiti sono informati dei loro diritti attraverso l'**informativa sul trattamento dei dati personali** (art. 13 del D.Lgs. 196/2003 c.d. Codice della *privacy*), che è il primo adempimento richiesto dalla normativa sulla *privacy*. L'informativa è stata definita a livello regionale. Si fa riferimento agli artt. 79 e 80 del Codice della *privacy* .
L'informativa viene in ogni caso personalizzata a seconda delle esigenze e procedure applicate dall'Istituto, tenendo conto dell'informativa-tipo che indica gli elementi essenziali di cui all'art. 13 del codice della *privacy*.

L'informativa è anche integrata con appositi cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi presso gli sportelli *front-office*, secondo quanto disposto dall'art. 80 del Codice della *privacy*.
Nel momento in cui il soggetto diviene maggiorenne, si deve provvedere ad informarlo direttamente, poiché in tale momento cessa di avere efficacia l'informativa in precedenza resa ai genitori, o ai soggetti cui spettava in generale la potestà genitoriale (art. 82 del Codice della privacy).
I modelli di Informativa sono consultabili sul sito *Internet* aziendale alla Voce Privacy: Informativa.

La normativa sulla *privacy* prevede la necessità di raccogliere il **Consenso al trattamento dei dati idonei a rivelare lo stato di salute (c.d. consenso privacy)** in tutti i casi in cui il cittadino accede alle nostre Strutture, previa consegna allo stesso dell'informativa ex art. 13 del Codice della privacy .
Il consenso privacy non deve confondersi con il consenso informato, necessario per sottoporre legittimamente un paziente a un intervento diagnostico-terapeutico, in modo che riceva un'informazione adeguata sullo scopo e sulla natura dell'intervento e sulle sue conseguenze e i suoi rischi).

Modalità di acquisizione del consenso privacy:

a) Il **consenso privacy "cartaceo"** antecedente al trattamento dei dati sanitari, che può essere sottoscritto dalla persona e/o dal sanitario che ha provveduto ad acquisirlo (in quest'ultimo tal caso il consenso viene manifestato oralmente e la dichiarazione viene documentata dall'operatore addetto – art. 81 del Codice della privacy), viene conservato nella cartella clinica e di essa è parte integrante: circa la tempistica segue le norme relative alla cartella clinica , quindi è conservata per tempo ancora illimitato.
b) Il **consenso privacy "informatizzato",** efficace a livello regionale (ossia in tutte le strutture sanitarie pubbliche e accreditate della Regione F.V.G) viene acquisito presso gli sportelli distrettuali mediante l'attivazione della Carta Regionale dei Servizi (CRS) ed è anch'esso illimitato, fino a manifestazione contraria dell'interessato.

Tutta la modulistica aziendale inerente il "consenso privacy" è consultabile e scaricabile sul sito *Intranet* aziendale alla Voce Privacy: Modulistica consenso.

Modalità di accesso ai dati

Istanza di accesso ai dati da parte dell'interessato, ex art. 7 del Codice della privacy.

Per "diritto di accesso ai dati" si intende il diritto di avere conferma della esistenza o meno dei propri dati personali e di avere la comunicazione in forma intellegibile dei dati stessi, intesi quindi come "informazioni detenute dalla Pubblica amministrazione", senza la forma di un documento amministrativo.

Il diritto di accesso ai dati personali da parte dello stesso titolare dei dati è esercitabile a titolo gratuito, salvo richiedere un contributo: a) in caso di riproduzione dei dati su speciale supporto; b) se la richiesta determina un notevole impiego di mezzi; c) quando non risulta confermata l'esistenza di dati che riguardano l'interessato.

L'Ufficio Relazioni con il Pubblico è sportello di *front-office* in grado di soddisfare le richieste di accesso e di conoscenza da parte degli interessati.

L'Istituto attua tutte le misure necessarie a facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 7 del Codice e predispone un apposito modulo rilasciato dall'URP, consultabile sul sito *Internet* aziendale alla Voce *Privacy: Fac-simile istanza ai sensi dell'art. 7 del D. Lgs. n. 196/2003* (allegato *D* Regolamento per la protezione dei dati personali).

Per quanto riguarda **l'accesso ai dati informatizzati**, l'Istituto ha disciplinato nel Documento Programmatico per la Sicurezza le modalità di erogazione e dismissione dei permessi d'accesso al fine di limitare l'accesso alle informazioni riguardanti gli utenti solamente al personale autorizzato.

Accesso ai documenti sanitari

Riguardo la richiesta di copia della documentazione sanitaria/cartella clinica da parte di persona diversa dall'interessato, esso è consentito nei limiti in cui sia strettamente indispensabile, in presenza delle condizioni stabilite dalla Legge 241/90, dall'art. 60 del Codice della privacy e dal **Regolamento aziendale per l'esercizio del diritto di accesso,** consultabile sul sito Intranet aziendale *Regolamento accesso documenti.*

Valutazione delle richieste di accesso da parte di terzi:

Per quanto riguarda la valutazione delle richieste di accesso da parte di terzi, occorre prestare attenzione sia alla L. 241/90 in materia di accesso ai documenti amministrativi (artt. 22 e ss.) che al D.Lgs. 196/2003 che fa riferimento alle richieste di accesso ai dati/informazioni (non quindi ai documenti), che possono essere sensibili, sanitari e giudiziari (artt. 59 e 60 del Codice della privacy).

La richiesta di accesso da parte di terzi richiede l'adozione di adempimenti e il rispetto di cautele, obblighi e limiti previsti dalla L. 241/90, dal regolamento di attuazione D.P.R. 184/2006 e dal D.Lgs. 196/2003, che appaiono condizionati dalla diversa natura delle informazioni di cui si richiede la conoscibilità:

Accesso ai dati di persona deceduta:
Se la persona alla quale si riferiscono i dati è deceduta, i diritti di accesso di cui all'art. 7 del Codice della privacy possono essere esercitati:
: a) da chi ha un interesse proprio; b) da chi agisce a tutela dell'interessato; c) da chi agisce per ragioni familiari meritevoli di protezione, ai sensi di quanto disposto all'art. 9, comma 3 del Codice stesso (es. gli eredi del defunto o chi rivendica la qualità di erede ed è stato estromesso dal testamento).

Accesso ai dati sensibili e giudiziari di terzi:
L'accesso a documenti contenenti dati sensibili o giudiziari relativi a terzi, in presenza delle condizioni stabilite dalla Legge 241/90, dal Regolamento che disciplina l'accesso di cui al D.P.R. 184/2006 e dal Regolamento aziendale per l'esercizio del diritto di accesso, è consentito nei limiti in cui sia "strettamente indispensabile": in tal caso, l'eventuale accoglimento di tale richiesta potrà - eventualmente (rientra nell'ambito del potere discrezionale dell'Amministrazione) essere limitato alla sola visione dei dati e non necessariamente anche all'estrazione di copia, in base al combinato disposto degli articoli 25, comma 3 e 24, comma 7 della L.241/90 con l'art. 22 del codice della *privacy.*
L'art. 3 del DPR 184/2006, prevede l'obbligo della notifica di tale richiesta di accesso ai "controinteressati" (ossia ai soggetti che dall'esercizio del diritto di accesso vedrebbero compromesso il loro diritto alla riservatezza) mediante raccomandata. con avviso di ricevimento, al fine di consentire a quest'ultimi di poter presentare motivata opposizione (anche per via telematica) entro dieci giorni dalla ricezione della richiesta stessa.

Accesso ai dati sanitari o attinenti alla vita sessuale di terzi:
Se il documento contiene **dati idonei a rivelare lo stato di salute o la vita sessuale di terzi**, la richiesta deve essere motivata dall'esigenza di tutelare un diritto di rango almeno pari a quello dell'interessato, cioè consistente in un diritto della personalità o in altro diritto o libertà fondamentale ed inviolabile (v. art. 60 del Codice della *privacy*).
La pubblica amministrazione è chiamata quindi a porre in essere una valutazione avente ad oggetto la verifica della parità di rango tra i diritti del contro-interessato (alla riservatezza, alla salute) e il diritto che si intende far valere con la richiesta di accesso considerata (cioè non il diritto di difesa ma il "diritto sottostante che si intende curare o difendere in sede di giudizio").

Accesso ai dati personali "comuni" di terzi (nome, cognome, indirizzo, codice fiscale ecc.)
Ove i **dati personali** di cui si richiede l'accesso sono di natura "comune" (diversi dai dati sensibili e giudiziari) troverà applicazione l'art.19, comma 3 del codice della *privacy*, che prevede la comunicazione a terzi solo se tale operazione è espressamente prevista da legge o regolamento.

Accesso ai documenti di terzi
Se invece il richiedente ha necessità di accedere a documenti di terzi occorre verificare se il soggetto richiedente vuol far valere un proprio interesse giuridico, in applicazione della L.241/90 e del regolamento di attuazione DPR 184/2006. In tal caso l'Istituto accoglierà la richiesta nei limiti di ciò che è "strettamente necessario" (consentendo anche l'estrazione di copia), previa notifica ai controinteressati ex. art. 3 del D.P.R. 184/2006.

In ogni caso, qualora l'Istituto ritenga di dover accogliere l'istanza di accesso, occorre effettuare una valutazione concreta su quali informazioni, fra quelle contenute nei documenti oggetto della richiesta, debbano essere comunicate e quali siano, invece, eccedenti rispetto allo scopo perseguito con l'accesso.

Documento Programmatico sulla Sicurezza (D.P.S.)
La conservazione e la salvaguardia dei dati personali sensibili e giudiziari dell'Istituto trattati mediante strumenti elettronici è regolamentata dal Documento Programmatico sulla Sicurezza, in conformità a quanto previsto dall'art.34, comma 1, lettera g) del Codice della privacy e dall'allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza".
Esso è aggiornato entro il 31 marzo di ogni anno ed è conservato presso il Protocollo Generale.
Riguardo agli **Amministratori di Sistema** (richiamati nel D.P.S.), la loro nomina è prevista dalla vigente normativa sulla *privacy* e in particolare in applicazione al Provvedimento del Garante del 27 novembre 2008, e vanno prescelti tra il personale abilitato all'accesso alle risorse informatiche e telematiche aziendali, al fine di legittimare questi ultimi ad operare nell'ambito dei profili di autorizzazione loro attribuiti, data la delicatezza e peculiarità delle loro mansioni e la necessità di prestare massima attenzione ai rischi e alle criticità relativi alla protezione dei dati.
L'elenco degli Amministratori di Sistema è riportato nel sito *Intranet* aziendale alla Voce *Privacy: elenco Amministratori di Sistema.*

5. PROCEDURE

La procedura inerente l'informazione, il consenso al trattamento e la comunicazione dei dati a terzi in ambito sanitario, sia con riferimento alla prestazione ambulatoriale che in regime di ricovero è indicata nel documento ***"Procedura operativa per il consenso privacy"***, comprensivo della relativa modulistica.
La modulistica è comunque consultabile nel sito *Intranet alla* Voce *Consenso*

6. RESPONSABILITA'

L'Istituto, quale Titolare del trattamento dei dati è responsabile nel definire le scelte organizzative e le modalità operative in materia di sicurezza nel trattamento dei dati personali, che vengono specificate nel Documento Programmatico sulla Sicurezza (D.P.S.), in conformità a quanto previsto dall'art. 34, comma 1, lettera *g)* del Codice e dall'allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza", nel caso di trattamento di dati personali sensibili e giudiziari mediante strumenti elettronici.

Tutti i professionisti ed operatori dell'Istituto sono a conoscenza e si impegnano a rispettare, nell'espletamento delle proprie attività, i diritti alla *Privacy* degli utenti nel pieno rispetto della Normativa e delle Leggi in vigore. A tale scopo ricevono e sottoscrivono un'apposita nomina a Responsabile o ad Incaricato dei trattamenti (v. Regolamento per la protezione dati personali)

consultabile nel sito Intranet aziendale alla Voce *Privacy*), assumendosene la piena responsabilità in ogni sede e seguono corsi obbligatori di formazione.

I **Responsabili del trattamento dei dati** devono garantire il rispetto delle misure minime di sicurezza, descritte nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" del Codice della privacy; la loro mancata adozione implica un illecito penale e comporta le sanzioni di cui all'art. 169 del Codice stesso.
Gli **Incaricati per il trattamento** dei dati devono attenersi alle disposizioni scritte del Responsabile.
Sia i Responsabili che gli Incaricati sono tenuti, oltre che al rispetto della Legge sulla *Privacy*, anche al *Segreto professionale* ed al *segreto d'ufficio*.

7. MODALITA' ESECUTIVE

Per una corretta comunicazione / informazione dei dati personali è necessario seguire i criteri e le regole di comportamento previste dal Codice *privacy*, tra i quali:

1. la richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa solamente nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge;
2. la comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato dal titolare o dal responsabile (v. art. 84 del Codice della *privacy*);
3. l'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Istitutoche possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia;
4. in ogni caso occorre porre in essere procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparto o strutture, indicativa dell'esistenza di un particolare stato di salute;
5. per poter usufruire delle prestazioni diagnostico/terapeutiche necessarie per la tutela della salute, all'utente che accede ai servizi sanitari e socio-sanitari dell'Istituto è necessario prestare il proprio consenso al trattamento dei dati personali, previa acquisizione dell'Informativa;
6. il personale addetto alle informazioni può fornire informazioni circa la presenza del paziente, salvo parere contrario da parte di quest'ultimo. E', pertanto, necessario che il degente/paziente autorizzi l'eventuale trasmissione ai parenti delle informazioni relative al suo stato di salute;
7. occorre osservare l'art. 83 del Codice della *privacy*, che prevede l'adozione di misure per il rispetto dei diritti del paziente quali ".....distanze di cortesia, modalità per appelli in sala di attesa, certezze e cautele nelle informazioni telefoniche del paziente e nelle informazioni sui ricoverati";
8. Particolarissima tutela deve essere riservata alle cartelle cliniche, ivi comprese quelle infermieristiche, sia con riferimento alla loro tenuta e conservazione che alle modalità di accesso alle stesse.

Tali adempimenti tutelano l'Istituto e gli operatori da responsabilità civili e/o penali derivanti da eventuali azioni promosse dall'utente/paziente (es.ricorsi, reclami o segnalazioni al Garante o all'Autorità Giudiziaria.). L'Istituto ha la possibilità di evitare ogni responsabilità solo dimostrando di aver adottato "tutte le misure idonee ad evitare il danno", ossia tutte quelle soluzioni e adempimenti che la normativa *privacy* prevede per il rispetto dei diritti degli utenti/pazienti.

A tal fine, l'Istituto provvede alla:

1. definizione delle procedure per: a) l'acquisizione del consenso *privacy;* b) il rilascio/accesso di dati/informazioni a terzi; c) la gestione delle istanze degli interessati per l'esercizio dei diritti ex art. 7 del Codice privacy;
2. standardizzazione della modulistica prevista per le procedure suddette;
3. revisione/aggiornamento costante dell'informativa ex art. 13 del Codice della *privacy,* da fornire obbligatoriamente all'interessato ai fini del la trasparenza dei trattamenti, nonché della modulistica, sotto il profilo dei contenuti tecnico - normativi;
4. organizzazione di corsi di formazione sul tema della *privacy* e della riservatezza per il personale, per una corretta e aggiornata applicazione della normativa in materia;
5. adozione di misure di sicurezza idonee a garantire la protezione dei dati e ridurre i rischi di perdita, distruzione, cancellazione anche accidentale dei dati stessi, di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità di raccolta.

8. RIFERIMENTI NORMATIVI e DOCUMENTI AZIENDALI

- D.Lgs. n. 196 del 30.06.2003 "Codice in materia di protezione dei dati personali"
- Provvedimenti del Garante per la protezione dei dati personali (reperibili sul sito *www.garanteprivacy.it*)
- Documento Programmatico della Sicurezza (DPS),
- Regolamento per il trattamento dei dati sensibili e giudiziari, approvato dalla Regione F.V.G., con Decr. Pres. Reg. 12 maggio 2006, n.0146/Pres. (consultabile sul sito Intranet aziendale alla Voce Privacy)
- Regolamento per l'esercizio del diritto di accesso ai documenti, (consultabile sul sito Intranet aziendale alla Voce Regolamenti)
- Regolamento per la protezione dei dati (consultabile sul sito Intranet aziendale alla Voce Privacy e Regolamenti)

9. DESTINATARI

-Tutto il personale e, più in generale, tutti gli operatori dell'Istituto;

-L'interessato al trattamento (paziente, utente, ditta aggiudicataria ecc.).

Ogni trattamento di dati personali consiste in un rapporto che si instaura tra titolare e interessato.
- L'interessato ha il potere di controllare i trattamenti svolti dall'Istituto che lo riguardano, esercitando in qualsiasi momento i diritti di cui all'art. 7 del Codice della privacy, che costituiscono diritti pieni ed esclusivi, con obbligo di risposta per l'Azienda, salvo i casi previsti dall'art. 8 del codice della *privacy*.
- L'interessato può far valere i diritti (considerati in via alternativa) presentando ricorso al Garante ovvero all'Autorità Giurisdizionale Ordinaria, la quale ha giurisdizione esclusiva per quanto concerne ogni questione attinente al codice della *privacy*.