ISTITUTO NAZIONALE TUMORI
IRCCS – Fondazione Pascale

Regolamento per la protezione dei dati personali in attuazione del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali".

INDICE

INTRODUZIONE

Nel presentare questo Regolamento, traendo insegnamento dall'esperienza di altre Aziende Sanitarie Italiane e soprattutto dalle difficoltà incontrate dalle stesse per promuovere la cultura della privacy, è opportuno chiarire cosa esso non è:

- *non è una normativa ulteriore rispetto a quella nazionale;*
- *non rappresenta una diminutio dell'autonomia gestionale dei singoli dirigenti;*
- *non si prospetta come un nuovo carico di lavoro per gli operatori della sanità.*

Il Regolamento aziendale sulla privacy è uno strumento di applicazione del D.L.vo 30 giugno 2003 n. 196 "codice in materia di protezione di dati personali", un atto dovuto e doveroso.
Le istruzioni in esso contenute intendono corroborare l'azione dirigenziale lasciandone intatta l'autonomia.

La attenzione posta dal Legislatore in materia di privacy è dovuta alla agevole, ma non banale considerazione, che attraverso un rispetto sostanziale e non formale dei dati della persona, si può ottenere un risultato importante: la tutela della dignità della persona.
Questo aspetto è ancora più evidente se le regole sulla privacy si applicano in una realtà particolare come quella sanitaria, che utilizza e conserva dati riferiti alla salute delle persone, dati non a caso definiti sensibili.

Un efficace rispetto delle regole che vengono dettate dalla Legge sulla privacy prevede un impegno organizzativo all'interno di ogni struttura aziendale.
E' necessario un sistema aziendale che presieda e governi la materia della privacy.
E' importante che le norme sulla privacy vengano applicate e non siano viste solamente come un ulteriore impaccio burocratico, ma come miglioramento della qualità del servizio offerto all'utenza.
Proprio nella speranza di fornire un impulso ed un sostegno a questa tensione al miglioramento e nella consapevolezza del forte impatto che la Legge sulla privacy inevitabilmente produce su una organizzazione dalla complessità elevata come quella dell'Istituto Fondazione G. Pascale, il Regolamento, unitamente al breve manuale sulle cautele da adottare ad esso allegato, intende contribuire al crearsi di tutte quelle relazioni necessarie per il corretto uso delle informazioni.

TITOLO I

PRINCIPI GENERALI

Articolo 1
Oggetto ed Ambito di applicazione

1. Il presente Regolamento contiene disposizioni attuative del D. Lgs. n. 196/2003 recante il "Codice in materia di protezione dei dati personali" (di seguito indicato come Codice) nell'ambito delle strutture e servizi dell'Istituto Fondazione Pascale di Napoli, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Istituto Fondazione Pascale.

Articolo 2
Definizioni

1. *Ai fini del presente Regolamento, come previsto dall'art. 4 del Codice, si intende per:*

a) ***«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 di dati, anche se non registrati in una banca di dati;*

b) ***«dato personale»****, qualunque informazione relativa a persona fisica, persona giuridica, Ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

c) ***«dati identificativi»****, i dati personali che permettono l'identificazione diretta dell'interessato;*

d) ***«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;*

e) ***«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;

f) ***«Titolare»****, 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, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;*

g) ***«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;*

h) ***«incaricati»****, le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;*

i) ***«interessato»****, la persona fisica, la persona giuridica, l'Ente o l'associazione cui si riferiscono i dati personali;*

l) ***«garante»****, l'autorità istituita dalla Legge sulla privacy;*

m) ***«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;*

n) ***«diffusione»****, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*

o) ***«dato anonimo»****, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

p) ***«blocco»****, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;*

q) ***«banca di dati»****, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;*

2. Ai fini del presente regolamento si intende altresì per:

a) ***«Referente aziendale per la privacy»*** *il soggetto, Dirigente individuato in ambito aziendale, che 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 sulla privacy;*

b) ***«Consulente informatico per la privacy»*** *il soggetto, Dirigente informatico individuato in ambito aziendale, che fornisce al Referente ed ai Responsabili del trattamento il necessario supporto informatico;*

*c) **«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 di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;*

*d) **«strumenti elettronici»**, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;*

*e) **«autenticazione informatica»**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.*

TITOLO II
SOGGETTI

Articolo 3
Soggetti autorizzati

1. Nel rispetto di quanto previsto dal Codice il trattamento dei dati è ammesso solo da parte dei soggetti di seguito indicati:
- Titolare;
- Responsabili del trattamento dei dati;
- Incaricati.
2. L'Istituto non consente il trattamento dei dati da parte di personale non autorizzato.

Articolo 4
Titolare del trattamento

1. Il Titolare del trattamento dei dati è l'Istituto Nazionale per lo Studio e la Cura dei Tumori - Fondazione Giovanni Pascale.

2. Con il supporto del Referente aziendale per la privacy di cui al successivo art. 9, il Titolare adempie gli obblighi previsti dalla normativa nazionale e dalle disposizioni regionali in materia di riservatezza dei dati personali nonché dal presente Regolamento ed in particolare:

a) effettua la notificazione al Garante ai sensi dell'articolo 37 del Codice;
b) richiede al Garante, qualora sia necessaria, l'autorizzazione al trattamento di dati sensibili;
c) assolve all'obbligo di nominare i Responsabili del trattamento dando le necessarie istruzioni per la corretta gestione e tutela dei dati personali.

Articolo 5
Responsabili del trattamento

1. I Responsabili del trattamento dei dati vengono designati con nota scritta dal Titolare, Istituto Nazionale per lo Studio e la Cura dei Tumori - Fondazione Giovanni Pascale, nella persona del suo legale rappresentante il Direttore Generale.

2. I Responsabili del trattamento dei dati sono individuati fra soggetti che per esperienza, capacità ed affidabilità, forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e che siano titolari:

- *di un incarico di responsabilità di unità operativa complessa;*
- *di un incarico di responsabilità di unità operativa dipartimentale;*
- *di un incarico di referenza di uffici dotati di autonomia organizzativa e decisionale.*

3. Il Responsabile del trattamento dei dati deve attenersi alle istruzioni impartite dal Titolare nell'atto di nomina ed osservare e far osservare le misure precauzionali individuate nel Documento Programmatico per la Sicurezza dei dati personali elaborato dall'Istituto.

4. In particolare il Responsabile collabora con il Referente provvedendo:
a) a fornire ogni informazione richiesta;
b) a comunicare tempestivamente ogni notizia rilevante ai fini della tutela della riservatezza;
c) a comunicare tempestivamente al Referente l'inizio di ogni nuovo trattamento dei dati nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza;
d) a trasmettere entro il mese di febbraio di ogni anno la relazione sulle misure di sicurezza di cui al successivo art. 19, comma 2, lett. c.

5. Il Responsabile ha l'obbligo di nominare formalmente come incaricati le persone fisiche (dipendenti dell'Istituto, soggetti con incarico libero professionale ai sensi dell'art. 7 del D. Lgs. n. 165/2001, soggetti ammessi allo svolgimento del tirocinio o della frequenza volontaria o che fruiscono di istituti similari) che nell'ambito dei trattamenti aziendali di sua diretta competenza effettuano operazioni di trattamento di dati personali.

6. Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al proprio settore di competenza.

7. La funzione di Responsabile del trattamento dei dati è attribuita personalmente e non è suscettibile di delega.

8. Il Referente aziendale per la privacy provvede a tenere l'elenco completo ed aggiornato dei Responsabili del trattamento dati in ambito aziendale.

9. A tale scopo l'Unità Operativa Gestione Risorse Umane deve partecipare tempestivamente al Referente per la privacy gli atti di attribuzione di responsabilità di strutture organizzative ed ogni eventuale successiva variazione intervenuta.

Articolo 6
Responsabili esterni
(outsourcing)

1. In tutti i contratti o convenzioni, con cui l'Istituto affida a terzi (Enti, organismi, associazioni di volontariato, persone fisiche, strutture private accreditate, società di persone o di capitali, studi legali) attività che comportano il trattamento di dati personali, deve essere inserita la clausola di garanzia con la quale il soggetto esterno si assume i seguenti obblighi:

a) trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto;

b) adempiere agli obblighi previsti dal Codice per la protezione dei dati personali;

c) rispettare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali;

d) informare sulle misure di sicurezza adottate e sulle eventuali successive modifiche;

e) informare immediatamente l'Istituto Fondazione Pascale in caso di situazioni anomale o di emergenze.

2. Con nota scritta l'Istituto Fondazione Pascale nomina il soggetto esterno come responsabile esterno dei trattamenti dei dati personali effettuati in forza del rapporto contrattuale o convenzionale.

3. A tal fine le strutture organizzative dell'Istituto che stipulino gli accordi e/o le convenzioni di cui al comma 1 hanno l'obbligo, entro 5 giorni dalla loro sottoscrizione, di trasmettere, debitamente compilato, al Referente aziendale per la privacy il modulo informativo allegato al presente Regolamento (All. A).

Articolo 7
Responsabili esterni
(studi osservazionali, sperimentazioni cliniche)

1. In tutti i contratti con cui l'Istituto si impegna a svolgere studi osservazionali o sperimentazioni cliniche, dovrà essere inserita apposita clausola di garanzia con la quale il soggetto esterno (società, istituti scientifici etc.), sponsor della ricerca si assume gli obblighi di:
a) trattare i dati ai soli fini della ricerca;
b) adempiere agli obblighi previsti dal Codice per la protezione dei dati personali;
c) rispettare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali;
d) informare sulle misure di sicurezza adottate e sulle eventuali successive modifiche;
e) informare immediatamente l'Istituto Fondazione Pascale in caso di situazioni anomale o di emergenze.

2. Con nota scritta l'Istituto Fondazione Pascale nomina il soggetto esterno come Responsabile esterno dei trattamenti dei dati personali effettuati in forza del rapporto

contrattuale anche ai fini di monitoraggio e/o ispezione secondo quanto previsto dalla legge.

3. Le strutture organizzative dell'Istituto Fondazione Pascale che stipulino i contratti di cui al comma 1, hanno l'obbligo, entro 5 giorni dalla loro sottoscrizione, di comunicare al Referente aziendale per la privacy quanto segue:
a) il trattamento di dati personali che lo studio o la sperimentazione comporta;
b) i dati identificativi ed il recapito dello sponsor (da nominare Responsabile esterno del trattamento);
c) la data della stipula del contratto.

Articolo 8
Incaricati del trattamento

1.Il Responsabile del trattamento nomina quali incaricati le persone fisiche che nell'ambito dei trattamenti di sua diretta competenza effettuano materialmente operazioni di trattamento di dati personali.

2. Tale nomina costituisce presupposto di liceità per il trattamento dei dati personali e/o sensibili in ambito aziendale da parte:

- dei dipendenti dell'Istituto (a tempo indeterminato o a tempo determinato);

- di soggetti con incarico libero professionale ai sensi dell'art. 7 del D. Lgs. n. 165/2001 che prestano la loro attività in ambito aziendale;

- di soggetti ammessi allo svolgimento del tirocinio o della frequenza volontaria o che fruiscono di istituti similari.

3. L'atto di nomina dell'incaricato contiene:
a) l'ambito dei trattamenti consentiti;
b) le istruzioni puntuali a cui gli incaricati devono attenersi scrupolosamente nel trattare i dati personali;
c) la prescrizione che gli incaricati abbiano accesso esclusivamente ai dati la cui conoscenza sia strettamente necessaria per l'espletamento dell'attività cui sono preposti;

4. L'atto di nomina degli incaricati deve essere redatto per iscritto preferibilmente utilizzando lo schema allegato al presente Regolamento (All. B).

5 . Il Responsabile notifica l'atto di nomina all'incaricato e, per conoscenza, al Referente aziendale per la privacy.

6 . I Responsabili del trattamento devono altresì comunicare tempestivamente al Referente aziendale per la privacy le eventuali modifiche successivamente intervenute quanto alla nomina degli incaricati.

7. Qualora il Responsabile debba designare più incaricati contemporaneamente si procede ad una sola designazione contenente più nominativi.

8. L'Azienda attua iniziative di formazione degli incaricati per consentire loro di acquisire conoscenze sul corretto trattamento dei dati.

TITOLO III
REFERENTE AZIENDALE PER LA PRIVACY E CONSULENTE INFORMATICO PER LA PRIVACY

Articolo 9
Referente aziendale per la privacy

1. Il Direttore Generale individua fra i dirigenti dell'Istituto il Referente Aziendale per la privacy (di seguito indicato come Referente).

2. Il Referente svolge i seguenti compiti:

a) 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;

b) provvede alla stesura del Documento Programmatico per la Sicurezza dei dati avvalendosi della necessaria collaborazione del Consulente informatico per la privacy e dell'apporto dei Responsabili del trattamento dei dati;

c) vigila sull'osservanza del presente Regolamento fornendo consulenza in ordine alle problematiche in tema di riservatezza;

d) tiene ed aggiorna il censimento dei trattamenti dei dati personali e/o sensibili sulla base delle comunicazioni effettuate dai Responsabili del trattamento;

e) promuove la cultura della privacy in ambito aziendale.

3. Nell'esercizio delle competenze di cui ai commi precedenti dovrà essere garantita al Referente la collaborazione di tutte le articolazioni organizzative dell'Istituto.

Articolo 10
Consulente informatico per la privacy

1. Il Direttore Generale nomina all'interno dell'Istituto il Consulente informatico per la privacy il quale:

a) collabora con il Referente aziendale per la privacy ai fini della stesura del Documento Programmatico per la Sicurezza (D.P.S.);

b) predispone la relazione in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici che costituisce parte integrante del Documento Programmatico per la Sicurezza;

c) fornisce al Referente ed ai Responsabili del trattamento il necessario supporto informatico;

d) su richiesta del Responsabile del trattamento attiva o disabilita le misure di sicurezza informatiche di cui al successivo art. 18.

Articolo 11
Comunicazioni preventive al Garante

1. Il Referente effettua le comunicazioni al Garante previste dall'art 39, comma 1, del Codice di seguito indicate:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento ed effettuata in qualunque forma anche mediante convenzione;

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo del Codice;

2. A tal fine è fatto obbligo a ciascun Responsabile interno od esterno all'Azienda di fornire al Referente gli elementi informativi necessari per effettuare le comunicazioni di cui sopra quale presupposto di legittimità del trattamento che si intende attivare.

TITOLO IV
Modalità di Trattamento

Articolo 12
Criteri per il trattamento dei dati personali

1. Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'Interessato.

2. Oggetto del trattamento devono essere i soli dati essenziali per svolgere attività istituzionali.

3. I Responsabili del trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità per le quali sono stati raccolti o successivamente trattati.

4. I dati che, anche a seguito delle verifiche, risultano eccedenti, non pertinenti o non necessari non potranno essere utilizzati, salvo che per l'eventuale conservazione prevista dalla legge dell'atto che li contiene.

5 . I Responsabili sono tenuti a comunicare dati personali ad altri Responsabili sia interni che esterni all'Istituto solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati anonimi o aggregati che impediscano di identificare l'interessato.

6 . I trattamenti di dati effettuati utilizzando le banche dati di diversi Titolari sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

TITOLO V
RAPPORTI CON L'UTENZA

Articolo 13
Informativa e visibilità del "Percorso privacy"

1. La persona fisica, giuridica, Ente o associazione cui si riferiscono i dati (interessato) o comunque la persona presso la quale sono raccolti i dati personali devono essere, previamente o al momento stesso della raccolta, informati oralmente o per iscritto, anche tramite affissione di appositi manifesti nei locali di accesso dell'utenza, in relazione a:

a) le finalità e le modalità del trattamento dei dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un'eventuale rifiuto nel fornire i dati;

d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui al successivo art. 14;

f) gli estremi identificativi dell'Istituto Fondazione Pascale in quanto Titolare.

2. Attraverso l'utilizzo di sistemi Intranet ed Internet l'Istituto attiva adeguate modalità di visibilità delle azioni poste in essere al suo interno in attuazione della normativa sulla riservatezza e degli indirizzi regionali in materia.

Articolo 14
Diritti dell'Interessato

1. Secondo quanto previsto dall'art. 7 del Codice l'interessato avvalendosi preferibilmente del modulo predisposto dall'Istituto (allegato C) ha il diritto di presentare all'Istituto istanza allo scopo:

a) di avere informazioni sull'esistenza o meno di propri dati personali in possesso dell'Istituto;

b) di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del Titolare, dei Responsabili, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentanti designati nel territorio dello Stato, di Responsabili o incaricati.

c) di ottenere l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati, 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;

d) di ottenere l'attestazione che le operazioni di cui alla lettera c) 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 per l'Istituto un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

2. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario, di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

3. Per dimostrare la propria identità l'interessato deve esibire o allegare all'istanza copia di un documento di riconoscimento secondo quanto previsto dall'art.9, comma quarto, del Codice.

4. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque ha un interesse proprio giuridicamente tutelato, o agisce a tutela del deceduto o per ragioni familiari meritevoli di protezione.

5 . Nell'esercizio dei diritti, l'interessato può conferire delega o procura scritta a persone fisiche, Enti, associazioni od organismi. In tal caso copia dell'atto deve essere esibita o allegata all'istanza.

6 . L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di una copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un Ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

7. Ai sensi dell'art. 10, commi 7 e 8 del Codice l'istanza di cui al presente articolo è soggetta a contributo qualora non risulti confermata l'esistenza di dati che riguardano l'interessato, nel caso di richiesta volta ad ottenere conferma dell'esistenza di propri dati personali presso la struttura organizzativa e/o di conoscere l'origine dei dati medesimi, nonché le finalità su cui si basa il trattamento e/o di conoscere la logica applicata.

8. La struttura organizzativa aziendale cui sia stata presentata l'istanza di cui al presente articolo deve trasmetterla al Referente immediatamente e comunque non oltre il termine di due giorni.

Articolo 15
Rapporti tra il diritto di accesso e il diritto alla privacy

1. L'accesso a documenti amministrativi contenenti dati personali di terzi, formati o detenuti da questo Istituto, resta disciplinato dalla Legge n. 241/1990.

2. Nel caso di dati idonei a rivelare lo stato di salute o la vita sessuale, l'accesso è consentito solo se la situazione giuridicamente tutelata che si intende salvaguardare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

3. In ogni caso le strutture organizzative che propongono una delibera o che adottano una determinazione dirigenziale verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dal Codice, che l'inclusione nel testo di dati personali sia realmente necessaria per le finalità proprie di ciascun provvedimento.

4. Laddove gli allegati delle delibere o delle determinazioni dirigenziali contengano dati sensibili tutelati dalla normativa sulla privacy, nel provvedimento dovrà essere evidenziato che l'allegato non viene pubblicato all'Albo, rimanendo depositato agli atti presso la struttura organizzativa, per esigenze di tutela della riservatezza dei destinatari del provvedimento o di terzi. Sull'allegato dovrà essere apposta la dizione "Riservato ai sensi delle vigenti norme sulla privacy".

TITOLO VI
Misure di sicurezza
Archivi

Articolo 16
Adozione delle misure minime di sicurezza

1. Il Titolare del trattamento dei dati, i Responsabili del trattamento dei dati e gli incaricati sono tenuti ad adottare le misure di sicurezza prescritte dalla normativa nazionale a tutela della privacy.

Articolo 17
Sicurezza degli archivi cartacei

1. L'accesso agli archivi aziendali deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura delle strutture ove gli archivi sono ubicati.

2. La responsabilità della conservazione e della sicurezza degli archivi amministrativi contenenti dati personali spetta al responsabile del trattamento che ha ad oggetto tali dati, fatta salva la disciplina aziendale in materia di archiviazione e deposito della documentazione amministrativa presso l'Archivio Generale dell'Istituto.

3. La responsabilità della conservazione e della sicurezza degli archivi delle cartelle cliniche è del Direttore della struttura sanitaria interessata.

4. Qualora la documentazione contenente dati personali sia archiviata presso una struttura accreditata che ha un rapporto di natura convenzionale con l'Istituto, il legale rappresentante della struttura medesima è responsabile della conservazione e della sicurezza dei dati e nella convenzione di affidamento del servizio dovranno essere previste:

a) un'apposita clausola di garanzia;

b) la facoltà per l'Istituto di accedere ai locali della struttura per verificare anche il rispetto delle prescrizioni del Codice privacy e del presente Regolamento.

Articolo 18
Adozione di misure di Sicurezza informatiche

1. Il trattamento di dati personali con l'ausilio di strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o ad un insieme di trattamenti.

2. Le credenziali di autenticazione possono consistere:

a) in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;

b) in un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o ad una parola chiave;

c) in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o ad una parola chiave.

3. Il Responsabile del trattamento assegna ad ogni incaricato una o più credenziali per l'autenticazione prescrivendogli di adottare le necessarie cautele per assicurare la

segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

4. Quando è prevista dal sistema di autenticazione, la parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

5 . Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

6 . Le credenziali di autenticazione sono disattivate se non utilizzate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica) o qualora l'incaricato abbia perso la qualità che consente l'accesso ai dati personali.

7. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, il Responsabile del trattamento fornisce agli incaricati specifiche disposizioni affinché sia assicurata la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata dal Responsabile del trattamento garantendo la relativa segretezza ed individuando preventivamente per iscritto i soggetti incaricati dal Responsabile del trattamento della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

8. E' utilizzato un sistema di autorizzazione quando per gli incaricati siano individuati profili di autorizzazione di ambito diverso.

9. 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.

10. Periodicamente, e comunque almeno annualmente, il Responsabile del trattamento verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti commi e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

12. Nell'atto di nomina il Responsabile del trattamento impartisce istruzioni agli incaricati per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento.

Articolo 19
Documento Programmatico per la Sicurezza

1. L'Istituto adotta, entro il 31 marzo di ogni anno, il Documento Programmatico della Sicurezza dei dati (D.P.S.).

2. Il Documento Programmatico della Sicurezza dei dati deve contenere:

a) l'Inventario Generale dei Trattamenti;

b) la distribuzione dei compiti e le responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi;

c) le relazioni dei Responsabili del trattamento sulle misure minime ed idonee adottate o da adottare sulla base dell'analisi dei rischi;

d) l'attività di formazione degli incaricati e dei Responsabili del trattamento al fine di un utilizzo consapevole delle informazioni gestite;

e) la raccolta delle informazioni in merito all'attività affidata all'esterno (outsourcing);

f) relazione del Consulente Informatico per la Privacy in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici;

g) la relazione dei Responsabili dei trattamenti circa le misure di sicurezza adottate per la sicurezza degli archivi cartacei di cui all'art. 17.

3. Il Referente predispone il Documento Programmatico per la Sicurezza avvalendosi del necessario apporto del Consulente Informatico per la privacy nonché della collaborazione di tutti i Responsabili del trattamento sia interni che esterni.

TITOLO VII
Censimento dei trattamenti dei dati personali e/o sensibili.

Articolo 20
L'Inventario Generale dei Trattamenti

1.L'istituto effettua il censimento dei trattamenti dei dati personali e/o sensibili.

2. L'Inventario Generale dei Trattamenti contiene la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative.

3. Di ogni trattamento censito sono individuati i seguenti elementi:
a) ambito di trasmissibilità dei dati;
b) natura personale e/o sensibile dei dati;
c) nominativo del Responsabile del trattamento;

d) personale incaricato del trattamento;
e) modalità informatica o cartacea con cui viene svolto il trattamento.

Articolo 21
Tenuta ed aggiornamento dell'Inventario Generale dei Trattamenti

1. L'Inventario Generale dei Trattamenti è tenuto a cura del Referente, il quale provvede ad aggiornarlo annualmente e comunque ogni volta che gli vengono comunicati da parte del Titolare o dei Responsabili del trattamento casi di:

a) attivazione di un nuovo trattamento o cessazione di un trattamento in essere;

b) variazione degli elementi di cui al comma 3 del precedente articolo 20 .

TITOLO VIII
NORME FINALI

Articolo 22
Norma di rinvio

Per quanto non previsto dal presente Regolamento trovano applicazione le disposizioni del D. Lgs. n. 196/2003.

Articolo 23
Abrogazioni

Sono abrogate tutte le disposizioni regolamentari dell'Istituto – Fondazione Pascale in contrasto con quelle previste dal presente Regolamento.

Articolo 24
Entrata in vigore

Il presente Regolamento, adottato con delibera del Direttore Generale, entra in vigore dal giorno della sua pubblicazione all'Albo dell'Istituto.