



REGOLAMENTO AZIENDALE

**per la protezione dei dati personali in attuazione del D.lgs. n. 196/2003
“Codice in materia di protezione dei dati personali”**

Azienda Unità Sanitaria di Taranto

Regolamento per la protezione dei dati personali in attuazione del D.lgs. n. 196/2003 “Codice in materia di protezione dei dati personali” e sue successive modificazioni ed integrazioni

INDICE

TITOLO I

Principi Generali

Articolo 1 Oggetto ed ambito di applicazione

Articolo 2 Definizioni

TITOLO II

Soggetti

Articolo 3 Soggetti autorizzati

Articolo 4 Titolare del trattamento

Articolo 5 Responsabili del trattamento

Articolo 6 Responsabili esterni (outsourcing)

Articolo 7 Responsabili esterni (studi osservazionali, sperimentazioni cliniche)

Articolo 8 Incaricati del trattamento

Articolo 9 Preposti al trattamento

TITOLO III

Ufficio Rapporti con il Garante e Tutela della Privacy (URGTP). Referente Privacy del Responsabile Struttura Complessa. Responsabile Sistemi Informativi Aziendali

Articolo 10 Ufficio Rapporti con il Garante e Tutela della Privacy (URGTP)

Articolo 11 Referente Privacy del Responsabile Struttura Complessa

Articolo 12 Responsabile Sistemi Informativi Aziendali

Articolo 13 Comunicazioni preventive al Garante

TITOLO IV

Modalità di trattamento

Articolo 14 “Criteri per il trattamento dei dati personali”

Articolo 15 Trattamento ai fini del lavoro

TITOLO V

Rapporti con l'utenza

Articolo 16 “Informativa e visibilità del Percorso privacy”

Articolo 17 “Diritti dell'Interessato”

Articolo 18 “Rapporti tra il diritto di accesso e il diritto alla privacy”

TITOLO VI

Misure di Sicurezza

Articolo 19 Modalità e riscontro all'interessato ed esercizio del suo diritto

Articolo 20 “Adozione delle misure minime di sicurezza”

Articolo 21 “Sicurezza degli archivi cartacei”

Articolo 22 “Adozione di misure di sicurezza informatiche”

Articolo 23 “Documento programmatico per la sicurezza”

TITOLO VII

Norme Finali

Articolo 24 “Norme di rinvio”

Articolo 25 “Entrata in vigore”

Azienda Unità Sanitaria di Taranto

Regolamento per la protezione dei dati personali in attuazione del D.lgs. n. 196/2003 “Codice in materia di protezione dei dati personali” e sue successive modificazioni ed integrazioni

TITOLO I

Principi Generali

Articolo 1 Oggetto ed ambito di applicazione

1. Il presente regolamento contiene le disposizioni attuative del D.lgs. n. 196/2003 recante il “Codice in materia di protezione dei dati personali” (di seguito indicato come Codice) e sue successive modificazioni ed integrazioni nell’ambito delle strutture, servizi e presidi dell’Azienda Unità Sanitaria Locale di Taranto, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone *fisiche e giuridiche*, con particolare riferimento alla riservatezza ed all’identità personale degli utenti e di tutti coloro che hanno rapporti con l’Azienda.
2. L’Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i 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.
3. L’Azienda adotta altresì le misure occorrenti per facilitare l’esercizio dei diritti dell’interessato ai sensi dell’art. 7 del D.lgs. 196/03.

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, effettuate 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 o 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'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 nov. 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 di cui all’articolo 153 del D.lgs. 196/2003, istituita dalla legge n. 675/1996.

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) Responsabile URGTP il soggetto, 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 anche in correlazione con l’accesso agli atti. Coordina l’attività dei singoli referenti dei responsabili del trattamento delle strutture complesse individuate con atto deliberativo del titolare.

b) Referente privacy del responsabile al trattamento e alla sicurezza dei dati della Struttura Complessa (P.O., Distretto, Dipartimento, Area ecc.) il soggetto, individuato dal Direttore Medico e/o Amministrativo della Struttura Complessa, che garantisce il supporto allo stesso per quanto riguarda gli adempimenti derivanti dalla normativa sulla privacy in diretta correlazione e secondo le disposizioni impartite dal responsabile URGTP;

b) Responsabile Sistemi Informativi Aziendali il soggetto che interagisce con la “Direzione aziendale, con i Direttori delle Aree competenti e delle strutture di staff “ per garantire la sicurezza informatica oltre a fornire al Responsabile URGTP, 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 di 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.
- ∞ Preposto al trattamento

2. L'Azienda non consente il trattamento dei dati da parte di personale non autorizzato salvo i casi di volta in volta che dovranno essere preventivamente concordati ed autorizzati dal Titolare e/o dal Responsabile del Trattamento sentito l'URGTP.

Articolo 4 Titolare del trattamento

1. Il Titolare del trattamento dei dati è l'Azienda Unità Sanitaria Locale Taranto nella persona del suo legale rappresentante.

2. Il Titolare, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza, si avvale operativamente del supporto, ognuno per la sua rispettiva competenza, dell'Ufficio Rapporti con il Garante e Tutela della Privacy (di seguito indicato come U.R.G.T.P.) di cui al successivo art. 10 e dell'Ufficio Sistemi Informativi Aziendali (di seguito indicato come S.I.A.) di cui al successivo art. 12, e provvede, nei casi previsti dalla legge :

a) ad assolvere l'obbligo di notificazione al Garante;

b) a richiedere, ove necessario, le autorizzazioni e ad effettuare le dovute comunicazioni all'Autorità Garante per il trattamento o la comunicazione dei dati;

c) a nominare i responsabili del trattamento dando le necessarie istruzioni per la corretta gestione e tutela dei dati personali;

d) ad adottare, per quanto di competenza, le misure necessarie a garantire la sicurezza dei dati personali, redigendo ed aggiornando il Documento Programmatico sulla Sicurezza;

e) ad impartire ai Responsabili le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza;

f) a verificare periodicamente l'osservanza dell'attività svolta dai Responsabili rispetto alle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

g) a provvedere alla formazione degli incaricati del trattamento dei dati personali, attraverso la previsione di interventi formativi , al fine di renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare medesimo.

Articolo 5 Responsabili del trattamento

1. I Responsabili del trattamento dei dati vengono designati con nota scritta dal Titolare.

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 struttura organizzativa;
- di un incarico di responsabilità di unità operativa professionale;
- 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 (o dal responsabile dell'URGTP) nell'atto di nomina ed osservare e far osservare le misure precauzionali individuate nel Documento Programmatico per la Sicurezza dei dati personali elaborato dall'Azienda.

4. In particolare il Responsabile si avvale operativamente del supporto del Referente privacy (di cui al successivo art.11) così come individuato nell'atto deliberativo che formalizza detto incarico, provvedendo:

- a) a fornire ogni informazione richiesta dal responsabile U.R.G.T.P. e S.I.A.;
- b) a comunicare tempestivamente ogni notizia rilevante ai fini della tutela della riservatezza;
- c) a comunicare tempestivamente al responsabile U.R.G.T.P. e S.I.A 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 adottate e su le eventuali integrazioni modificazioni o cancellazione delle banche dati.

5. Il Responsabile ha l'obbligo di nominare formalmente come incaricati le persone fisiche (dipendenti dell'Azienda) 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. L'U.R.G.T.P. provvede a tenere l'elenco completo ed aggiornato dei Responsabili del trattamento dati in ambito aziendale.

9. A tale scopo l'Area Gestione del Personale deve comunicare tempestivamente all'U.R.G.T.P. gli atti di attribuzione di responsabilità di strutture organizzative ed ogni eventuale successiva variazione intervenuta al fine di consentire a detto Ufficio la proposta di nomina di responsabile al trattamento.

Articolo 6 Responsabili esterni (outsourcing)

1. In tutti i contratti o convenzioni, con cui l'Azienda affida a terzi (Enti, organismi, associazioni di volontariato, persone fisiche, strutture private accreditate, società di persone o di capitali, studi legali) l'attività e/o servizi 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'Azienda Unità Sanitaria Locale Taranto in caso di situazioni anomale o di emergenze;
- f) comunicare all'URGTP lo stato di formazione del personale impiegato in materia di privacy.

2. Con nota scritta l'Azienda nomina, ai sensi dell'art. 29 del D.lgs. 196/03, 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'Azienda che stipulano i contratti e/o le convenzioni di cui al comma 1 hanno l'obbligo, entro 5 giorni dalla loro sottoscrizione, di trasmettere all'U.R.G.T.P. copia di tutta la documentazione afferente detto rapporto (ivi compresa atto deliberativo completo di allegati) al fine di predisporre la proposta di nomina di responsabile del trattamento da parte del titolare.

Articolo 7 Responsabili esterni

(studi osservazionali, sperimentazioni cliniche)

1. In tutti i contratti o convenzioni, con cui l'Azienda 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 assumono 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 successive modifiche;
- e) informare immediatamente l'Azienda Unità Sanitaria Locale Taranto o per essa l'URGTP in caso di situazioni anomale o di emergenze.

2. Con nota scritta l'Azienda nomina, ai sensi dell'art. 29 del D.lgs. 196/03, il soggetto esterno come Responsabile esterno dei trattamenti dei dati personali effettuati in forza del rapporto contrattuale anche ai fini del monitoraggio e/o ispezione secondo quanto previsto dalla legge.

3. A tal fine le strutture organizzative dell'Azienda, che stipulino i contratti o le convenzioni di cui al comma 1, hanno l'obbligo, entro 5 giorni dalla loro sottoscrizione, di trasmettere all'U.R.G.T.P. copia di tutta la documentazione afferente detto rapporto (ivi compresa atto deliberativo completo di allegati) ed in particolare quanto segue:

- a) il trattamento dei 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, con l'ausilio ed il supporto del Referente privacy della Struttura (ove indicato), nomina quali incaricati le persone fisiche che nell'ambito dei trattamenti di loro 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 di dette persone fisiche.

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.

5. Il Responsabile a mezzo del suo referente privacy (se individuato) 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, a mezzo del suo referente privacy (se individuato), all'URGTP 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.

Articolo 9 Preposti al trattamento.

Il preposto al trattamento è il soggetto a cui è affidato, nell'organizzazione di un servizio, il trattamento di una una o più banche dati sia in forma cartacea che informatica. Egli è individuato dall'incaricato al trattamento in occasione del monitoraggio delle banche dati presenti nello stesso servizio.

Titolo III

Ufficio Rapporti con il Garante e Tutela della Privacy (URGTP). Referente Privacy del Responsabile Struttura Complessa. Responsabile Sistemi Informativi Aziendali

Articolo 10 Ufficio Rapporti con il Garante e Tutela della Privacy (URGTP)

1. Ai fini del presente regolamento e della sua piena applicazione semplificata, il TITOLARE (rappresentante legale dell'Azienda), fermo restando la diretta vigilanza, indelegabile, stabilisce che gli adempimenti previsti dal codice in materia di protezione dei dati personali nonché gli orientamenti ed i provvedimenti emessi dal Garante dovrà essere svolto dall'Ufficio Rapporti con il Garante e Tutela della Privacy (URGTP).

L'URGTP è costituito dal suo responsabile e da tutti i referenti privacy indicati dai responsabili del trattamento e della riservatezza dei dati con lettera e con successivo atto formale da parte dello stesso TITOLARE.

2. L'URGTP 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 di protezione dei dati personali;
- b) provvede alla predisposizione degli atti necessari, ai fini dell'adempimento degli oneri previsti dalla normativa suddetta;
- c) provvede per la parte di sua spettanza (con esclusione di quella informatica e della sua sicurezza) alla stesura del Documento programmatico per la sicurezza dei dati, avvalendosi della necessaria collaborazione dei citati referenti privacy;
- d) vigila sull'osservanza del presente regolamento fornendo consulenza in ordine alle problematiche in tema di riservatezza;
- e) tiene ed aggiorna il censimento dei trattamenti dei dati personali e/o sensibili sulla base delle comunicazioni effettuate dai referenti privacy per conto dei Responsabili del trattamento;
- f) promuove in ambito aziendale la cultura della privacy e l'osservanza del regolamento aziendale sulla privacy, fornendo la necessaria consulenza in ordine alle problematiche in tema di riservatezza;
- g) promuove e coordina la formazione dei dipendenti in materia di privacy.

3. Nell'esercizio delle competenze di cui ai commi precedenti deve essere garantita all'URGTP la collaborazione di tutte le articolazioni organizzative dell'Azienda.

Articolo 11 Referente privacy

Il referente privacy del responsabile al trattamento e alla sicurezza dei dati della Struttura Complessa (P.O., Distretto, Dipartimento, Area ecc.), ove indicato, è il soggetto, individuato dal Direttore Medico e/o Amministrativo della Struttura Complessa, che garantisce il supporto allo stesso per gli adempimenti applicativi della normativa del codice e delle disposizioni del Garante, nei rapporti con altri soggetti pubblici o privati in diretta correlazione e secondo le disposizioni impartite dal responsabile URGTP. In particolare:

- accertare e verificare, sentito preventivamente il responsabile URGTP ed il responsabile al trattamento– a cui dovrà essere riferito periodicamente– la liceità ed il corretto utilizzo e trattamento, da parte degli operatori sanitari, dei dati sensibili; la conservazione e sicurezza degli stessi dati nonché, la osservanza delle disposizioni previste dalla normativa vigente in materia;

- proporre, sentito preventivamente l'URGTP, al Responsabile al trattamento e della sicurezza dei dati l'adozione di provvedimenti di richiamo, diffida e denuncia nei confronti degli incaricati del trattamento (anche nella loro qualità di responsabili di cui al documento programmatico) e dei suoi preposti per irregolare tenuta degli archivi e per un trattamento di dati in difformità ai dettami legislativi e/o del presente regolamento.

- comunicazione all'URGTP degli archivi esistenti; della creazione di nuove banche dati e/o della loro variazione, cessazione, integrazione e cancellazione.

- collaborare anche con gli incaricati ed i preposti e con altre figure individuate dal codice, al fine di fornire informazioni sugli aggiornamenti apportati in materia dal legislatore o per l'attività che il responsabile vorrà intraprendere o promuovere per l'espletamento dei compiti attribuiti dalla norma in conformità agli indirizzi dell'URGTP.

- verificare anche per disposizione dell'URGTP che il trattamento dei dati è esercitato osservando le regole della riservatezza e della segretezza.

- invio di copie di pareri e/o comunicati emessi da parte dell'URGTP.

- promuovere ogni iniziativa utile per evitare contenziosi e dissipare

disappunti da parte degli utenti e degli interessati contribuendo ad offrire loro ogni delucidazione e chiarimento sulle motivazioni del trattamento dei dati in possesso.

-ogni iniziativa utile per garantire la riservatezza, la segretezza e la sicurezza delle banche dati, sui dati contenuti e sul loro trattamento con particolare attenzione alla legge 241/90 e sue successive modificazioni ed integrazioni.

Articolo 12 Responsabile Sistemi Informativi Aziendali

1. Il rappresentante legale dell'Azienda (titolare) nomina all'interno dell'Azienda il Consulente informatico il quale:

- a) provvede, per quanto di propria competenza, alla stesura del Documento programmatico per la sicurezza;
- b) predispone la relazione in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici, che potrà costituire 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 in collaborazione con la società in outsourcing della gestione dei sistemi informatici aziendali.
- e) quant'altro stabilito dalla delibera del Direttore Generale n. 1825 del 5.09.2003 e sue successive integrazioni e/o modificazioni.

Articolo 13 Comunicazioni preventive al Garante

1. L'URGTP 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, 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'art. 110, primo periodo del Codice.

2. A tal fine è fatto obbligo a ciascun Responsabile interno o esterno, anche a mezzo dei loro referenti, all'Azienda di fornire all' URGTP 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 14 Criteri per il trattamento dei dati personali

1. Il trattamento dei dati (da parte del titolare, del responsabile, dell'incaricato, del preposto nonché da parte di tutti gli operatori) 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 dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni di trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati.
4. Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
5. 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.
6. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione prevista dalla legge dell'atto che li contiene.
7. I Responsabili sono tenuti a comunicare dati personali ad altri responsabili sia interni che esterni all'Azienda solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati anonimi o aggregati che impediscono di identificare l'interessato.
8. 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.

Articolo 15 Trattamento ai fini del lavoro

E' consentito, all'Azienda USL TARANTO, il trattamento dei dati che hanno finalità riferite alla instaurazione e gestione dei rapporti di lavoro. Sia "dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo , e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato". Secondo l'art.112, numero 2, del d.lgs. 196/03, sono ricompresi tra i trattamenti autorizzati quelli che l'Azienda USL TARANTO effettua per:

- a. "applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
- b. garantire le pari opportunità;
- c. accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
- d. adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;
- e. adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
- f. applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a

tipi di dati individuati specificatamente;

- g. svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
- h. comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
- i. salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;
- l. gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;
- m. applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale (in forma anonima);
- n. svolgere l'attività di indagine e ispezione presso soggetti pubblici (in forma anonima);
- o. valutare la qualità dei servizi resi e dei risultati conseguiti (in forma anonima)".

TITOLO V

Rapporti con l'utenza

Articolo 16 Informativa e visibilità del “Percorso privacy”

1. La persona fisica, giuridica, ente o associazione cui si riferiscono i dati (interessato =dipendente, utente, ricoverato ecc.=) o comunque la persona presso la quale sono raccolti i dati personali deve essere, previamente o al momento stesso della raccolta, informata 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 o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- e. i diritti di cui al successivo art. 17;
- f. gli estremi identificativi dell'Azienda in quanto titolare e del Responsabile al trattamento¹.

2. Attraverso l'utilizzo di sistemi Intranet ed Internet l'Azienda 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 nonché secondo il regolamento aziendale.

Articolo 17 Diritti dell'Interessato

1. Secondo quanto previsto dall'art. 7 del Codice l'interessato ha il diritto di presentare all'Azienda istanza allo scopo:

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

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 soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di Responsabili o Incaricati;

c) di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha 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'Azienda 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 ai fini di invio di materiale pubblicitario o 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 o associazioni od organismi. In tal caso copia dell'atto deve essere esibita o allegata all'istanza. Art. 13 D.lgs. 196/2003-

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 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.

Articolo 18 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 questa Azienda resta disciplinato dal regolamento aziendale per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi ai sensi della Legge 241/1990 e ss. mm. ed ii..

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 "seppure parte integrante e sostanziale", è depositato agli atti presso la struttura proponente dell'atto disposizione di chi ha interesse e ciò per esigenze di tutela della riservatezza dei destinatari del provvedimento o di terzi.

Articolo 19 Modalità e riscontro all'interessato ed esercizio del suo diritto

I diritti riconosciuti all'interessato, così come opportunamente richiamati nel precedente articolo, sono esercitati su semplice richiesta, anche verbale, direttamente al RESPONSABILE e/o ALL'INCARICATO i quali hanno il dovere di fornire idoneo riscontro.

Qualora la richiesta dell'interessato coinvolga più uffici essa dovrà essere rivolta, per il tramite dell'ufficio che l'ha ricevuta all'URGTP il quale entro 30 giorni dovrà fornire notizia mediante lo stesso responsabile e/o incaricato che ha provveduto ad accettarla ed istruirla e/o del suo referente privacy (ove indicato).

La richiesta così come inoltrata dall'interessato ed indirizzata al responsabile, incaricato della banca dati e/o direttamente all'URGTP può essere formulata anche mediante lettera raccomandata, telefax o posta elettronica o a mezzo di altro idoneo sistema che il Garante potrà ritenere opportuno.

Detta richiesta potrà essere rivolta dall'interessato –liberamente e senza costrizioni- anche verbalmente quando si tratti: a)dell'origine dei dati personali; b)delle finalità e modalità del trattamento; c)della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d)degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e)dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati (numero 2, precedente art.5).

La richiesta, di cui alle precedenti lettere, potrà essere rinnovata, per l'esistenza di giustificativi motivi, con intervallo non inferiore ai 90 giorni.

Fatta salva la facoltà spettante all'interessato circa la possibilità di farsi rappresentare per delega o procura da persone fisiche (anche di fiducia), enti, associazioni od organismi “i diritti di cui all'art. 7 (d.lgs.196/03) riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato e

per ragioni familiari meritevoli di protezione”.

Il responsabile, il preposto-incaricato, od altra figura rappresentante l’Azienda, ha il dovere di verificare “sulla base di idonei elementi di valutazione” l’identità dell’interessato. Quest’ultimo, infatti, dovrà esibire un documento di riconoscimento o se persona sua delegata deve esibire o allegare “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 (comma 4, art.9 d.lgs. 196/03)”.

IN PARTICOLARE: per garantire i diritti di cui agli artt. 6 e 7 del presente regolamento, l’Azienda USL TARANTO in qualità di titolare del trattamento, è tenuta a porre in essere misure atte: ad “agevolare l’accesso” ai dati in possesso dell’interessato anche a mezzo di programmi che snelliscono la ricerca; a “semplificare le modalità e a ridurre i tempi per il riscontro al richiedente”. Il riscontro alla richiesta dell’interessato, sia che essa si riferisca “ad un particolare trattamento o a specifici dati personali o categoria di dati”, dovrà comprendere tutti i dati personali oggetto del trattamento da parte dell’Azienda USL TARANTO salvo che i dati si riferiscano allo stato di salute che “possono essere resi noti all’interessato o a soggetti di cui all’art.82, comma 2, lett.a, d.lg.196/03 (“impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell’interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l’interessato”). Ciò da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall’interessato o da altro titolare (art.84 ,comma 1 d.lgs.196/03)”.

Quest’ultimo comma, non si applica se i dati trattati, ed in possesso del titolare, siano stati forniti precedentemente dall’interessato.

I dati così estratti possono essere comunicati verbalmente oppure, se richiesti , in forma scritta.

In tutti gli altri casi di riscontro all’interessato del trattamento dei dati personali da parte dell’Azienda non qui previsti, si applicano i dispositivi di cui ai numeri 4,5,6,7,8 e 9 dell’art.10 del d.lgs. 196/03.

I diritti dell’interessato (così come esplicitati nel precedente art.5) sulla richiesta della esistenza o meno dei dati personali che lo riguardano e

trattati dall'Azienda USL TARANTO non possono essere esercitati (ivi la possibilità di ricorrere al Garante ai sensi dell'art. 145 del d.lgs.196/03) qualora essi siano effettuati:

a) “in base alle disposizioni del decreto legge 3 maggio 1991, n.143, convertito, con modificazioni, dalla legge 5 luglio 1991 n. 197, e successive modificazioni, in materia di riciclaggio;

b) in base alle disposizioni del decreto legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n.172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'art.82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) ai sensi dell'art.24, comma 1, lettere f (casi nei quali può essere effettuato il trattamento senza consenso), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;

h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981 n.121.

Per i casi di cui alle precedenti lettere a), b), d), e) ed f) il Garante provvede nei modi e nei termini previsti dagli artt. 157,158 e 159 d.lgs.196/03 (accertamenti e controlli capo III) e nei modi di cui all'art.160 del citato decreto per i casi elencati nelle precedenti lettere c), g) ed h) anche su segnalazione dell'interessato.

TITOLO VI

Misure di sicurezza

Articolo 20 Adozione delle misure minime di sicurezza

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

In particolare il responsabile al trattamento, con il supporto del referente indicato, deve provvedere a:

- Controllare che il personale addetto rispetti il segreto professionale;
- Rispettare l'ordine di precedenza e di chiamata dell'utente (prescindendo dalla loro individuazione nominativa) in caso di prenotazione, di disbrighi amministrativi, di prestazione sanitarie ecc.;
- Istituire "apposite distanze di cortesia" non trascurando l'eventuale uso di idonei sistemi vocali e di segnalazione verticale ed orizzontale, nonché cartelli di avviso per rispetto delle distanze ai fini della privacy dell'utente;
- Prevenire, durante colloqui tra personale addetto ed utenze, che terzi possano venire a conoscenza di informazioni personali che rilevano lo stato di salute;
- Evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti ;
- Rispettare la dignità dell'interessato durante la prestazione medica e in ogni operazione di trattamento offrendo la disponibilità accompagnata da gentilezza e cortesia da parte dell'operatore intervenuto;
- Assicurarsi che le informazioni richieste sono date all'interessato o a terzi legittimati;
- Garantire una corretta informazione a terzi legittimati (familiari ecc.) sulla dislocazione degli interessati ospiti nell'ambito dei reparti e/o servizi offrendo a questi ultimi preventiva istruzione di dislocazione in occasione del ricovero; salvo il caso di formale dichiarazione di diniego da parte dell'interessato;
- Prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni che possano rivelare lo stato di salute dei ricoverati;
- Garantire la riservatezza dei dati e notizie in possesso di ogni Struttura Sanitaria ed Amministrativa, servizio ecc. da ogni intrusione, intolleranza e sproposita visione e consultazione anche da parte di personale non addetto; così come i preposti devono preoccuparsi di evitare ogni comunicazione verbale dei dati durante l'inserimento degli stessi nella banca dati corrispondente;

- Evitare che persone estranee, senza giusto motivo, sostino in ambienti di lavoro all'interno delle stesse strutture (soprattutto ospedaliere) in ore non consentite per la visita dei degenti o fuori dell'orario di ufficio (qualora si tratti del disbrigo di pratiche amministrative);

Articolo 21 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'Azienda.

3. La responsabilità della conservazione e della sicurezza degli archivi delle cartelle cliniche è del Direttore Medico dei Presidi Ospedalieri.

4. Qualora la documentazione contenente dati personali sia archiviata presso una struttura accreditata che ha un rapporto di natura convenzionale e/o contrattuale con l'Azienda, 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'Azienda di accedere ai locali della struttura per verificare anche il rispetto delle prescrizioni del Codice privacy e del presente Regolamento.

Articolo 22 Adozione di misure di Sicurezza informatiche

o Istruzioni circa l'uso della propria stazione di lavoro

Il personal computer o il terminale che è stato assegnato per lo svolgimento dei compiti di ufficio deve essere adoperato e custodito con attenzione.

L'incaricato nell'esercizio delle sue funzioni deve impegnarsi a:

- Attivare la password di BIOS e la password dello screensaver, tutto ciò al fine di evitare che terzi possano accedere al computer e carpirne i dati;
- tenere, nel limite del possibile, chiuso a chiave il proprio ufficio così da evitare indesiderati o indebiti accessi ai locali:
 - a.** in cui si svolge l'incarico assegnato
 - b.** in cui sono custoditi e trattati dati personali.
- non lasciare la propria postazione non presidiata per periodi lunghi
- chiudere la propria sessione di lavoro ogni volta che ci si assenta dall'ufficio
- evitare, durante la navigazione in Internet i seguenti comportamenti a rischio:
 - a.** trasmettere dati sensibili via e-mail;
 - b.** la navigazione su siti di hacking, cracking, ecc.;
 - c.** scaricare software da siti poco attendibili o non ufficiali e, comunque, senza prima avere avuto l'autorizzazione da parte dell'Amministratore di Sistema;
 - d.** inviare posta elettronica in formato "html" che è uno dei metodi più subdoli per veicolare contenuti virus, worm e frodi, senza necessità di file allegati;
 - e.** rispondere a messaggi di posta "non sollecitati", chiedendo di essere cancellati da quella lista di invio: in tal modo rischiate di fare il gioco di chi li ha spediti, facendogli capire che la vostra casella di posta è attiva;
 - f.** comunicare la vostra e-mail a siti ai quali non siete interessati per fini istituzionali.
- eseguire periodicamente la pulizia del disco da cookies, file temporanei, etc;
- eseguire periodicamente salvataggi dei dati (documenti, database etc.) presenti sulla stazione di lavoro;

- [] [] [] [] [] [] porre particolare attenzione nell'utilizzo di pendrive, floppy che possano essere infetti da virus, accertandosi di avere installato Antivirus Centralizzato o altro antivirus attivo e non scaduto;
- [] [] [] [] [] [] non esitare a proporre al Responsabile del trattamento particolari accorgimenti in tema di sicurezza.

o **Istruzioni circa l'utilizzo della password**

Tutti gli incaricati del trattamento dei dati personali accedono ai sistemi informativi per mezzo di codici identificativi personali (in seguito indicati User-id) e password personali.

- [] [] [] [] [] [] la password è segreta e non deve essere comunicata ad altri;
- [] [] [] [] [] [] la password va custodita con diligenza e riservatezza;
- [] [] [] [] [] [] l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una sua rivelazione.

User-id e password iniziali sono assegnati dal custode delle password. Il custode delle password è identificato con il gestore dei singoli Sistemi Informativi.

Lo User-id e la password vanno richiesti al custode delle password attraverso la compilazione di un apposito modulo e secondo criteri a seconda dei diversi Sistemi informativi a cui l'utente dovrà accedere. Il Modulo così compilato andrà consegnato in busta chiusa al custode delle password, il quale provvede alla sua conservazione assicurandone la riservatezza.

Ogni sei mesi (tre nel caso di trattamento di dati sensibili) ciascun incaricato provvede a richiedere la sostituzione della propria password attraverso la compilazione dello stesso modulo che va consegnato al custode delle password con le stesse modalità suindicate.

Articolo 23 Documento Programmatico sulla Sicurezza dei dati

Ai sensi e per gli effetti degli articoli da 33 a 36 del D.lgs. 196/03 e dell'Allegato B del medesimo codice, l'Azienda aggiorna annualmente il Documento Programmatico sulla Sicurezza dei dati sulla base dell'analisi dei rischi che incombono sui medesimi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento, delle misure in essere e da adottare, nonché dei criteri e delle modalità di ripristino della disponibilità dei dati.

TITOLO VIII

Norme finali

Articolo 24 Norme di rinvio

Per quanto non previsto dal presente regolamento trovano applicazione le disposizioni del D.lgs. n. 196/2003 e ss. mm. ed ii.

Articolo 25 Entrata in vigore

Il presente regolamento **annulla il precedente adottato con delibera direttoriale n. del ed entra in vigore dall'adozione dell'atto deliberativo del TITOLARE (rappresentante legale) che ne sancirà l'approvazione.**

