

## CONTENUTI DEL DOCUMENTO

1.	TITOLO.....	2
2.	CONDUTTORE.....	2
3.	MODIFICHE ALLE REVISIONI PRECEDENTI.....	2
4.	OBIETTIVI.....	2
5.	AMBITO DI APPLICAZIONE.....	3
6.	SEQUENZA DELLE ATTIVITA'.....	3
6.1	Informazioni introduttive.....	3
6.2	Trattamenti effettuati in Azienda.....	5
6.3	Funzioni e responsabilità identificate.....	5
6.4	Informativa e consenso al trattamento dei dati degli utenti.....	13
6.5	Informativa e consenso al trattamento dei dati dei dipendenti e dei fornitori.....	15
6.6	Misure strutturali per la protezione dei dati personali.....	16
6.7	Misure organizzative generali per la protezione dei dati personali.....	16
6.8	Istruzioni specifiche relative al trattamento dei dati sensibili.....	19
6.9	Misure per la protezione dei dati trattati con l'ausilio di strumenti elettronici.....	21
6.10	Misure strutturali e organizzative per tutelare la riservatezza degli utenti.....	22
6.11	Politica per la Privacy.....	23
6.12	Rapporti con il Garante.....	23
7.	DOCUMENTI E REGISTRAZIONI CORRELATI.....	23
8.	ELENCO DI DISTRIBUZIONE.....	24
9.	DIFFUSIONE.....	24

stesura	verifica dei contenuti e approvazione	verifica di conformità ed emissione
Commissione Privacy	Direttore Generale	Rappresentante della Direzione

## 1. TITOLO

PG 542.05 - Sicurezza dei Dati e Tutela della Privacy.

### 1.1 Descrizione sintetica

In applicazione del DLgs 196/2003 (Codice), la presente Procedura descrive le modalità identificate dalla Direzione Generale dell'Azienda per attuare la protezione dei dati personali degli utenti, dei fornitori e dei dipendenti e per tutelare la riservatezza degli utenti. Vengono specificate le necessarie responsabilità e definite le modalità operative per adempiere in modo efficace alle disposizioni del Codice.

La presente Procedura è stata stesa in applicazione del Codice, viene integrata, per quanto concerne la descrizione della politica di sicurezza e delle misure adottate e previste dall'Azienda in relazione al processo di trattamento dei dati con strumenti elettronici, dal Documento di Programmazione sulla Sicurezza (DPS) e sostituisce la Procedura Generale PG 424.03 - Gestione della Sicurezza nel Trattamento dei Dati Personali, la cui stesura era stata determinata dalla emanazione del DPR 318/1999, ora abrogato.

Per aspetti specifici si fa riferimento a ulteriori Procedure Generali.

Inoltre la presente Procedura, messa a disposizione di tutti gli operatori sui luoghi di lavoro e, in copia elettronica, sul sito Intranet aziendale, assolve anche all'obbligo, attribuito al Titolare e al Responsabile dall'articolo 30, comma 1 del Codice, di impartire istruzioni agli Incaricati. Le indicazioni fornite dalla presente Procedura potranno essere integrate da indicazioni più specifiche per determinati ambiti di lavoro, impartite direttamente dai relativi Responsabili del trattamento dei dati.

## 2. CONDUTTORE

Direttore Generale.

## 3. MODIFICHE ALLE REVISIONI PRECEDENTI

Revisione	Emissione	Modifiche apportate
0	21/10/2005	Trattandosi della prima stesura, non esistono modifiche da segnalare.
1	gg/mm/aaaa	Nella riunione del 16/01/2007 la Commissione Privacy ha approvato le seguenti modifiche: <ul style="list-style-type: none"> <li>- Al § 6.2.2 sono state inserite informazioni sul Regolamento per il trattamento dei dati sensibili e giudiziari adottato dalla Regione Piemonte</li> <li>- L'elenco dei Responsabili del trattamento dei dati al § 6.3.2 è stato modificato</li> <li>- Le modalità di designazione degli Incaricati, previste al § 6.3.3, sono state semplificate</li> <li>- E' stato aggiunto il § 6.3.10</li> <li>- E' stato modificato il § 6.4.1 relativo all'Informativa</li> <li>- E' stato modificato il § 6.4.2 relativo al Consenso, adottando le modalità semplificate previste dal Codice</li> <li>- E' stato modificato il § 6.7.3 relativo alle Istruzioni generali sul trattamento dei dati</li> <li>- E' stato modificato il § 6.8 relativo alle Istruzioni specifiche sul trattamento dei dati.</li> </ul> Su indicazione della Direzione Generale è stata modificata la composizione della Commissione Privacy al § 6.3.9. La modulistica è stata aggiornata.

## 4. OBIETTIVI

- ⊕ Dare attuazione al Codice in materia di protezione dei dati personali (Decreto Legislativo 30/06/2003 n. 196, pubblicato su GU 29/07/2003 n. 174, SO n. 123)
- ⊕ Impartire agli operatori le istruzioni generali necessarie a garantire la riservatezza degli utenti e la sicurezza nel trattamento dei dati personali.

## **5 AMBITO DI APPLICAZIONE**

La presente Procedura si applica a tutte le attività svolte in Azienda per le quali sia necessario effettuare trattamenti di dati personali e/o sensibili relativamente a dipendenti, fornitori o utenti e, per quanto riguarda la tutela della privacy, a tutte le attività per le quali sia previsto un qualunque tipo di contatto con gli utenti.

## **6. SEQUENZA DELLE ATTIVITA'**

### **6.1 Informazioni introduttive**

#### **6.1.1 GENERALITÀ**

Il Codice in materia di protezione dei dati personali integra, razionalizza e coordina in un nuovo "Codice" gli elementi di tutta la normativa fino ad ora emessa al riguardo, introducendo anche importanti innovazioni che tengono conto della "giurisprudenza" del Garante e della Direttiva comunitaria 2002/58/CE sulla riservatezza nelle comunicazioni elettroniche; dal 01/01/2004, con l'entrata in vigore del Codice, sono abrogate tutte le norme precedenti, compresi la Legge 675/1996 e il DPR 318/1999.

Strutturalmente il Codice è diviso in tre parti (complessivamente 186 articoli). La prima è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato. La seconda è la parte speciale dedicata a specifici settori, quali ad esempio l'ambito sanitario, il lavoro e la previdenza sociale, le comunicazioni elettroniche. La terza parte affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante. Sono inoltre allegati al Codice:

- ⊕ Il codice di deontologia dei giornalisti (Allegato A1)
- ⊕ Il codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici (Allegato A2)
- ⊕ Il codice di deontologia per il trattamento dei dati personali a scopi statistici in ambito Sistan (Allegato A3)
- ⊕ Il codice di deontologia e di buona condotta per il trattamento dei dati personali a scopi statistici e scientifici (Allegato A4)
- ⊕ Il codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (Allegato A5)
- ⊕ Il disciplinare tecnico in materia di misure minime di sicurezza (Allegato B)
- ⊕ I trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia (Allegato C).

Saranno altresì allegati, via via che verranno adottati, altri codici di deontologia e di buona condotta attualmente in corso di predisposizione.

Il Codice ha la finalità di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Tali garanzie sono estese anche ai diritti delle persone giuridiche (società private e pubbliche) e di ogni altro ente o organizzazione.

## 6.1.2 GLOSSARIO

Ai fini della presente Procedura vengono utilizzate le seguenti definizioni, la maggior parte delle quali sono tratte dall'articolo 4 del Codice; quelle seguite da un asterisco sono tratte da altre fonti.

**Autenticazione informatica:** L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità

**Autorizzazione informatica:** vedi **Sistema di autorizzazione**

**Banca dati:** Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità, dislocate in uno o più siti.

**Blocco:** La conservazione di dati personali con sospensione temporanea di ogni altra operazione del 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.

**Credenziali di autenticazione:** I dati ed i dispositivi in possesso di una persona da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

**Crittografia** \*: Sistema che consente di rendere maggiore la sicurezza di un file tramite codifica. Una volta che un file è stato crittografato, per poter essere letto deve essere decrittografato.

**Dati giudiziari:** I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u) del DPR 14/11/2002 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.

**Dati identificativi:** I dati personali che permettono l'identificazione diretta dell'interessato.

**Dati sensibili:** I dati personali idonei a rilevare 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 rilevare lo stato di salute e la vita sessuale.

**Dato anonimo:** Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

**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.

**Diffusione:** Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Garante:** L'autorità di cui all'articolo 153 del Codice.

**Incaricati:** Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

**Interessato:** La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

**Parola chiave:** Componente di una credenziale di autenticazione associata ad una persona e a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

**Profilo di autorizzazione:** L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

**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.

**Separazione dei dati elettronici** \*: I dati sensibili sono archiviati in tabelle/file separati da quelli contenenti i dati identificativi. Dove la separazione è realizzata, anche nel caso di intrusione nella banca dati il riconoscimento di un soggetto non sarebbe possibile senza una conoscenza completa delle relazioni tra gli oggetti componenti la struttura logica del database.

**Sistema di autorizzazione:** L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

**Strumenti elettronici:** Gli elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

**Titolare:** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitariamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

**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.

## **6.2 Trattamenti effettuati in Azienda**

### 6.2.1 TIPOLOGIE DI DATI TRATTATI

L'Azienda effettua trattamenti sulle seguenti categorie di dati:

- ⊕ Dati personali relativi ai cittadini assistibili
- ⊕ Dati personali e sanitari relativi alle prestazioni erogate
- ⊕ Dati personali e sanitari relativi a donatori e riceventi di organi e tessuti
- ⊕ Dati personali relativi a fornitori di beni e servizi
- ⊕ Dati giudiziari relativi a fornitori di beni e servizi
- ⊕ Dati personali relativi al personale dipendente o cessato dal servizio
- ⊕ Dati sensibili e giudiziari relativi al personale dipendente o cessato dal servizio
- ⊕ Dati personali, sensibili e giudiziari relativi a parenti di personale dipendente
- ⊕ Dati relativi alla video-sorveglianza di alcune aree dell'Azienda
- ⊕ Dati relativi al traffico telefonico fisso e mobile delle utenze aziendali
- ⊕ RegISTRAZIONI delle conversazioni telefoniche in entrata e in uscita del centralino della Centrale Operativa 118.

### 6.2.2 REGOLAMENTO PER IL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI

In attuazione dell'articolo 20, comma 2 del Codice, della Direttiva del Ministero Funzione Pubblica dell'11/02/2005 e del Provvedimento del Garante del 30/06/2005, con DPGR 3/R del 11/05/2006 la Regione Piemonte ha emesso il "Regolamento per il trattamento dei dati personali sensibili e giudiziari". L'allegato A contiene le schede relative ai trattamenti di competenza della Regione, degli enti e agenzie regionali, degli enti controllati e vigilati dalla Regione. L'allegato B contiene le schede relative ai trattamenti di competenza delle Aziende sanitarie. Per ciascuna tipologia di trattamento vengono dettagliati: le finalità di interesse pubblico perseguite, i tipi di dati sensibili trattati e le principali operazioni eseguite. Per le finalità di interesse pubblico perseguite e le operazioni eseguite vengono specificate, quando previsto, le fonti normative di riferimento. L'allegato B del DPGR 3/R è stato modificato con DPGR 14/R del 04/12/2006. Ai fini dei trattamenti eseguiti presso l'Azienda Ospedaliera CTO/Maria Adelaide risultano applicabili le schede elencate in Tabella 1.

Nella individuazione dell'ambito del trattamento per gli Incaricati (vedi § 6.3.3), i Responsabili del trattamento dei dati si attengono alle indicazioni fornite dal Regolamento regionale, e in particolare dalle schede sopra riportate. Il testo integrale degli Allegati al Regolamento sono pubblicati sul sito Intranet dell'Azienda (Sistema Documentale, sezione Regolamenti aziendali).

## **6.3 Funzioni e responsabilità identificate**

### 6.3.0 GENERALITÀ

Rispetto ai dati personali il Codice identifica alcune figure cui sono affidate specifiche responsabilità. Altre figure e le relative responsabilità sono state identificate all'interno dell'Azienda per opportunità particolari, sempre legate al trattamento dei dati personali.

### 6.3.1 TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati della Azienda CTO/Maria Adelaide è il Direttore Generale, il quale:

- ⊕ Approvando la presente Procedura Generale definisce le modalità del trattamento dei dati e il profilo di sicurezza caratteristico della Azienda
- ⊕ Nomina i Responsabili del trattamento dei dati e gli Amministratori di sistema mediante lettera di incarico (moduli MOD PG 542.05-13, -10, -11, -12).

TABELLA 1. TRATTAMENTI EFFETTUATI DALL'AZIENDA OSPEDALIERA CTO/MARIA ADELAIDE PREVISTI NELL'AMBITO DEL DPGR REGIONE PIEMONTE 3/R DEL 11/05/2006

Allegato	Scheda	Titolo
A	1	Nomine e designazioni da parte della regione, delle aziende sanitarie, degli enti e agenzie regionali, degli altri enti vigilati e controllati dalla regione
A	2	Instaurazione e gestione del rapporto di lavoro del personale inserito a vario titolo presso l'ente regionale, le aziende sanitarie, gli enti e le agenzie regionali e gli altri enti vigilati e controllati dalla regione, compreso collocamento obbligatorio, assicurazioni integrative
A	3	Attività sanzionatoria e di tutela amministrativa e giudiziaria riguardante l'ente regionale, le aziende sanitarie, gli enti e le agenzie regionali e gli altri enti vigilati e controllati dalla regione
A	12	Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
B	1	Tutela dei rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
B	2	Sorveglianza epidemiologica delle malattie infettive e diffuse e delle tossinfezioni alimentari
B	3	Vaccinazioni e verifica assolvimento obbligo vaccinale
B	4	Programmi di diagnosi precoce
B	12	Assistenza integrativa (fornitura di prodotti dietetici a categorie particolari e di presidi sanitari a soggetti affetti da diabete mellito)
B	17	Attività amministrativa, programmatoria, gestionale e di valutazione relativa alla assistenza in regime di ricovero ospedaliero e domiciliare
B	18	Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività immuno-trasfusionale
B	19	Attività amministrativa, programmatoria, gestionale e di valutazione concernente il trapianto d'organi
B	20	Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza
B	21	Assistenza specialistica ambulatoriale e riabilitazione
B	25	Assistenza farmaceutica territoriale e ospedaliera
B	26	Sperimentazione clinica dei medicinali
B	27	Farmacovigilanza e rilevazioni reazioni avverse a vaccino
B	28	Erogazione a totale carico del SSN, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dalla Commissione Unica del Farmaco
B	30	Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'assistenza ai neuropatici cronici in trattamento dialitico
B	33	Attività medico-legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego, idoneità allo svolgimento di mansioni lavorative, controllo dello stato di malattia di dipendenti pubblici e privati)
B	35	Attività medico-legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
B	36	Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza da causa di servizio
B	37	Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari
B	39	Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
B	41	Video-sorveglianza con finalità di sicurezza e protezione di beni e persone

### 6.3.2 RESPONSABILI DEL TRATTAMENTO DEI DATI

Quali Responsabili del trattamento dei dati sono identificati:

- ⊕ I Direttori di Struttura Complessa, sanitaria o amministrativa
- ⊕ I Responsabili di Struttura Semplice o Ufficio non aggregati ad una Struttura Complessa e a cui, in base all'organigramma aziendale, siano state attribuite unità di personale dedicato.

Con Deliberazione 516/DG/2004/UAI del 30/06/2004 il Direttore Generale ha nominato i Responsabili del trattamento dei dati, identificandoli nei Direttori delle Strutture Complesse e Semplici. In data 13/08/2004 ciascun Responsabile del trattamento dei dati identificato ha ricevuto copia della Delibera in oggetto e lettera di incarico a firma del Direttore Generale.

Con Deliberazione 719/DG/2005/UAI del 21/10/2005 è stata rettificata la Deliberazione 516/DG/2004/UAI del 30/06/2004 ed approvata la presente Procedura in revisione 0. Il Direttore Generale ha provveduto nuovamente, mediante lettera di incarico nominativa (modulo MOD PG 542.05-13), a nominare Responsabili dei trattamenti dei dati della propria Struttura i Direttori di Struttura Complessa e i Responsabili di Struttura Semplice non aggregata a Struttura Complessa e a cui siano state attribuite unità di personale dedicato, con le responsabilità specificate al presente paragrafo. Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

In occasione della nomina di nuovi Direttori di SC o di nuovi Responsabili di Struttura Semplice non aggregata a Struttura Complessa, gli stessi vengono nominati Responsabili dei trattamenti dei dati della propria Struttura mediante lettera di incarico nominativa (modulo MOD PG 542.05-13). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

A seguito di ogni modifica dell'assetto del personale dell'Azienda che comporti modifiche delle funzioni in ambito aziendale, il Direttore della SC Amministrazione del Personale informa il Direttore della SC Sistemi Informativi affinché questi provveda ad aggiornare le credenziali di autenticazione sui sistemi informatici e/o l'elenco dei Responsabili del trattamento dei dati pubblicato sul sito Intranet dell'Azienda.

I Responsabili del trattamento dei dati hanno la responsabilità di rispettare e far rispettare da parte degli Incaricati le disposizioni contenute nel Codice, nella presente Procedura e nel Documento di Programmazione sulla Sicurezza, ed in particolare:

- a. Nominano formalmente gli Incaricati del trattamento tramite lettera di incarico (modulo MOD PG 542.05-14), fornendo loro, se necessario, istruzioni aggiuntive rispetto a quelle contenute nella presente Procedura (vedi anche § 6.3.3, terzo capoverso)
- b. Comunicano alla Commissione Privacy l'inizio di ogni nuovo trattamento, la cessazione o la modifica di un trattamento già in essere all'interno del proprio settore di competenza, al fine di permettere l'aggiornamento dell'anagrafe dei trattamenti di dati personali dell'Azienda
- c. Predispongono tutte le misure organizzative idonee a garantire la sicurezza dei trattamenti effettuati mediante strumenti non automatizzati
- d. Richiedono all'Amministratore di Procedura o di rete i codici identificativi personali e le password per il trattamento di dati effettuato con sistemi automatizzati, da consegnare agli Incaricati (vedi Procedura Generale PG 63\_.15)
- e. Forniscono agli Incaricati le istruzioni per la corretta selezione e l'utilizzo delle password e vigilano sul loro corretto utilizzo
- f. Collaborano con l'Amministratore di Procedura affinché gli Incaricati abbiano accesso, all'interno delle banche dati, solo ai dati di rispettiva competenza
- g. Comunicano trimestralmente all'Amministratore di Procedura le eventuali variazioni di mansione relative agli Incaricati
- h. Comunicano tempestivamente alla Commissione Privacy ogni questione ritenuta rilevante ai fini della applicazione della normativa sulla privacy
- i. Forniscono alla Commissione Privacy le informazioni richieste.

Gli archivi cartacei sono tenuti e custoditi a cura dei Responsabili del trattamento di competenza.

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 perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

I Responsabili del trattamento sono tenuti a comunicare dati personali e/o sensibili 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 impediscano di identificare l'interessato.

Le verifiche sull'osservanza da parte dei Responsabili del trattamento delle disposizioni contenute nella presente Procedura e nel Documento di Programmazione sulla Sicurezza (vedi § 6.9.1) sono effettuate nell'ambito degli Audit periodici del SGQ previsti al § 8.2.2 del Manuale Aziendale del SGQ.

La qualità di Responsabile del trattamento viene inoltre attribuita ad enti, organismi e soggetti esterni all'Azienda e a strutture accreditate cui siano delegate attività di competenza dell'Azienda che comportano, per la loro esecuzione, l'utilizzo di dati personali e/o sensibili e con esclusivo riferimento alle connesse operazioni di trattamento di dati.

Nel caso di documentazione archiviata presso ditta convenzionata, il legale rappresentante della medesima è individuato dal Direttore Generale quale Responsabile del trattamento dei dati.

Nei contratti di affidamento di attività o di servizi a strutture esterne all'Azienda (*outsourcing*) viene inserita apposita clausola di garanzia con la quale il soggetto accreditato o affidatario si impegna alla osservanza delle norme di legge sulla protezione dei dati personali e ad osservare quanto disposto dall'Azienda in materia di trattamento di dati personali effettuati in forza del rapporto contrattuale. Il Riquadro 1 riporta la clausola da inserire nei contratti.

### 6.3.3 INCARICATI DEL TRATTAMENTO DEI DATI

Gli Incaricati sono identificati in tutti coloro che materialmente effettuano le operazioni di trattamento di dati personali e/o sensibili. Non si configurano quali Incaricati i soggetti che trattano esclusivamente dati statistici.

Con Deliberazione 441/C/98/UAI del 18/03/1998 tutto il personale dipendente è stato nominato Incaricato del trattamento dei dati; per il Personale assunto dopo il 18/03/1998 la designazione ad Incaricato del trattamento avviene mediante espressa previsione contenuta nel contratto di assunzione. Nel contratto di assunzione viene prevista solo una clausola relativa all'obbligo di rispettare la normativa sul trattamento dei dati sulla base delle indicazioni fornite dal Responsabile del trattamento dei dati cui il dipendente è assegnato; la designazione avviene a carico del Responsabile del trattamento dei dati.

I Responsabili del trattamento dei dati possono avvalersi di due distinte modalità di designazione degli Incaricati:

- ⊕ Redazione di formale lettera di incarico (modulo MOD PG 542.05-14), con la indicazione delle tipologie di dati che l'Incaricato è autorizzato a trattare ed eventuali istruzioni aggiuntive rispetto a quelle fornite ai §§ 6.7 e 6.8. Le lettere di incarico, controfirmate dagli Incaricati, sono conservate a cura del Responsabile. Al variare delle funzioni assegnate il Responsabile dovrà predisporre un nuovo atto di nomina.
- ⊕ Usufruendo della modalità semplificata prevista dall'articolo 30 del Codice, Il Responsabile può predisporre un documento che definisca l'ambito di trattamento previsto all'interno della Struttura, eventualmente specificandolo per ciascuna qualifica di personale che opera nella Struttura. Il Responsabile deve comunque dare evidenza della presa visione del documento da parte di tutti gli Incaricati e il documento deve essere sempre disponibile sui luoghi di lavoro.

Gli Incaricati sono formati in modo tale da permettere loro di acquisire conoscenza sul corretto trattamento dei dati e sono tenuti ad eseguire i trattamenti secondo le disposizioni ricevute.

All'atto di stipula dei contratti, i consulenti dell'Azienda vengono contestualmente nominati Incaricati, con la specifica indicazione delle tipologie di dati che sono autorizzati a trattare. Il Riquadro 2 seguente riporta la clausola da inserire nei contratti.

#### 6.3.4 AMMINISTRATORI DI SISTEMA

Relativamente al trattamento dei dati con strumenti elettronici, a livello aziendale sono individuate tre tipologie di strumenti elettronici e quattro distinte tipologie di Amministratori di sistema.

##### Tipologie di strumenti elettronici

- ⊕ Procedura informatica centralizzata, in genere trasversale alle diverse SC, gestita dalla SC Sistemi Informativi, e i cui dati risiedono su server centralizzati della sala server aziendale presso il Presidio CTO
- ⊕ Procedura informatica locale e/o dipartimentale acquisita e gestita da una specifica SC
- ⊕ Procedura di controllo operativo e monitoraggio delle apparecchiature elettromedicali e dispositivi medici, sia quando la procedura risiede direttamente sull'elettromedicale/dispositivo medico, sia quando risiede su specifica apparecchiatura informatica collegata all'elettromedicale/dispositivo medico stesso.

##### Amministratori di sistema

- ⊕ Amministratore della rete aziendale, che gestisce le modalità di accesso alla rete aziendale, sia dall'interno che dall'esterno, e le relative abilitazioni ai servizi di rete. Le credenziali di accesso alla rete non comportano, di per sé, accesso ai dati trattati dall'Azienda. Possono tuttavia essere utilizzate, secondo le indicazioni dei Responsabili del trattamento, per consentire l'accesso a dati trattati con strumenti elettronici.
- ⊕ Amministratore di server, ovvero dell'elaboratore su cui risiedono le basi dati e le funzioni di elaborazione centralizzata di una procedura informatica centralizzata acquisita e gestita dalla SC Sistemi Informativi o locale acquisita e gestita da una specifica SC
- ⊕ Amministratore di procedura informatica, che gestisce le modalità di accesso e le abilitazioni ad operare degli Incaricati, in relazione ai trattamenti che si avvalgono di una procedura informatica centralizzata acquisita e gestita dalla SC sistemi informativi o locale acquisita e gestita da una specifica SC
- ⊕ Amministratore di procedura per il controllo operativo e monitoraggio delle apparecchiature elettromedicali/dispositivi medici.

#### 6.3.5 AMMINISTRATORE DI RETE AZIENDALE

Le funzioni e le responsabilità dell'Amministratore di Rete sono:

- a. Conservare i codici e le password di accesso per la configurazione degli apparati attivi per la trasmissione dei dati sulla rete
- b. Rilasciare i codici e le password da assegnare alle eventuali parti terze abilitate al collegamento al sistema informatizzato centrale aziendale dall'esterno (ad esempio i fornitori di procedure informatiche) ai fini di consentire l'erogazione dell'assistenza da remoto. Per le modalità operative identificate vedi Procedura Generale PG 63\_.15
- c. Definire ed aggiornare, compatibilmente con le soluzioni disponibili sul mercato, gli strumenti tecnologici atti a proteggere la rete aziendale da intrusioni e accessi non autorizzati
- d. Garantire il corretto funzionamento degli strumenti tecnologici acquisiti a tal fine
- e. Svolgere controlli atti a rilevare eventuali accessi alla rete non autorizzati
- f. Mantenere aggiornata la documentazione tecnica relativa alla configurazione hardware e software della rete e degli strumenti di sicurezza.

L'Amministratore di rete è nominato, su proposta del Direttore della SC Sistemi Informativi, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Diretto-

re Generale mediante lettera di incarico (modulo MOD PG 542.05-10). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

#### 6.3.6 AMMINISTRATORE DI SERVER

Le funzioni e le responsabilità dell'Amministratore di Server sono:

- a. Conservare i codici e le password di accesso per la configurazione del server e l'accesso alle funzioni sistemiche di manutenzione della medesima
- b. Rilasciare i codici e le password da assegnare alle eventuali terze parti abilitate al collegamento al server dall'esterno (ad esempio i fornitori di procedure informatiche) ai fini di consentire l'erogazione dell'assistenza da remoto. Per le modalità operative identificate vedi Procedura Generale PG 63\_.15
- c. Definire ed aggiornare, compatibilmente con le soluzioni messe a disposizione dal produttore del software di sistema in uso, gli strumenti tecnologici atti a proteggere il server da intrusioni e accessi non autorizzati
- d. Garantire il corretto funzionamento degli strumenti tecnologici acquisiti a tal fine
- e. Svolgere controlli atti a rilevare eventuali accessi non autorizzati al server
- f. Garantire l'effettuazione delle operazioni di salvataggio dei data base presenti sul server, la non accessibilità di tali copie da parte di terzi non autorizzati, l'efficacia delle procedure di ripristino in caso di danneggiamento dei dati, la distruzione delle copie non più necessarie per le finalità di ripristino (vedi Procedura Generale PG 63\_.14).

L'Amministratore di Server di una procedura informatica acquisita e gestita centralmente dalla SC sistemi informativi è nominato, su proposta del Direttore della SC Sistemi Informativi, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Direttore Generale mediante lettera di incarico (modulo MOD PG 542.05-11). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

L'Amministratore di Server di una procedura informatica locale e/o dipartimentale acquisita e gestita da una specifica SC è nominato, su proposta del Direttore della SC che gestisce il server locale presso i singoli servizi, e quindi non gestito centralmente dalla SC Sistemi Informativi, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Direttore Generale mediante lettera di incarico (modulo MOD PG 542.05-11). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

#### 6.3.7 AMMINISTRATORE DI PROCEDURA

Le funzioni e le responsabilità dell'Amministratore di Procedura sono:

- a. Conservare i codici e le password di accesso all'intera base dati della procedura e all'insieme completo delle funzionalità di elaborazione gestite dalla medesima
- b. Rilasciare i codici e le password da assegnare agli Incaricati dei trattamenti che utilizzano la procedura. Per le modalità operative identificate vedi Procedura Generale PG 63\_.15
- c. Assegnare a ciascun Incaricato il profilo di utenza corrispondente alle sole funzionalità necessarie alla attività istituzionale svolta dal medesimo
- d. Garantire, compatibilmente con le caratteristiche tecnologiche della procedura gestita, che i codici di accesso assegnati non siano utilizzabili da più stazioni di lavoro contemporaneamente e che le relative password siano modificabili e conosciute soltanto dagli Incaricati che ne sono in possesso

RIQUADRO 1. CLAUSOLA DA INSERIRE NEI CONTRATTI DI AFFIDAMENTO DI ATTIVITÀ O SERVIZI IN GESTIONE ALL'ESTERNO

All'atto dell'affidamento del Servizio, il Fornitore è nominato Responsabile del trattamento dei dati utilizzati per l'espletamento delle attività oggetto del contratto. Nel trattamento di tali dati, il Fornitore dovrà adempiere a tutte le misure previste dal DLgs. 196/2003, nonché a tutte le successive modifiche e/o integrazioni eventualmente introdotte nel periodo di vigenza contrattuale. Il Fornitore dovrà inoltre adeguarsi alle politiche di sicurezza adottate dall'Azienda, ancorché queste siano maggiormente impegnative rispetto alle misure minime previste dalla normativa vigente.

Se tenuto alla redazione del DPS, in relazione al trattamento dei dati relativi all'esecuzione del contratto con l'Azienda, il Fornitore dovrà produrre, prima dell'inizio delle attività, una certificazione di avvenuta adozione del DPS e di avvenuta adozione di tutte le misure di sicurezza minime richieste dall'allegato B in conformità al DLgs 196/2003. L'Azienda si riserva il diritto di richiedere in visione ed eventualmente richiedere di modificare il DPS prodotto dal Fornitore in relazione al trattamento dei dati oggetto del contratto, in qualsiasi momento della vigenza contrattuale, e il Fornitore si impegna all'attuazione di tali modifiche e alla implementazione delle misure di sicurezza eventualmente discendenti da tali modifiche, con tutti gli oneri relativi a proprio carico e nei tempi indicati dall'Azienda. L'Azienda si riserva il diritto di verificare l'applicazione delle misure di sicurezza previste dalla normativa vigente e dal DPS del Fornitore presso i locali in cui si effettuano le attività di trattamento dei dati oggetto del contratto, ancorché queste si svolgano al di fuori dei locali dell'Azienda ed il fornitore si impegna a mettere in atto tutte le misure necessarie all'espletamento di tali verifiche.

Alla cessazione del contratto, nel caso in cui i dati trattati in esecuzione del servizio affidato non siano già in possesso dell'Azienda, o lo siano solo in modo parziale, il Fornitore consegnerà all'Azienda tutti i dati in proprio possesso o l'integrazione a quelli già eventualmente nella disponibilità dell'Azienda, relativi al contratto scaduto, sia che questi siano su supporto cartaceo che informatico. I dati dovranno essere consegnati in versione intelligibile e, nel caso si tratti di integrazioni, in modo tale che sia possibile una facile correlazione con quelli già in possesso dell'Azienda. Nel caso di dati consegnati su supporto informatico, questo dovrà essere leggibile con i comuni dispositivi informatici e con le specifiche del formato logico utilizzato per la memorizzazione dei dati. Quando i formati logici non siano di uso comune, ed in particolare quando siano utilizzati formati proprietari, il Fornitore dovrà rendere disponibili, senza alcun onere per l'Azienda, le procedure software applicative di lettura dei formati con i quali sono consegnati i dati, nonché gli eventuali software di base necessari. Nel caso i dati siano ritenuti non più necessari all'espletamento della propria attività, l'Azienda può rinunciare alla consegna dei dati da parte del Fornitore mediante comunicazione scritta. In seguito a verifica positiva della leggibilità dei dati trasmessi o alla rinuncia della consegna dei dati da parte del Fornitore, l'Azienda comunicherà per iscritto al Fornitore di procedere alla distruzione di tutti gli archivi in suo possesso, indicando il termine entro il quale effettuare tale operazione, se la conservazione di tali dati non sia prescritta al fornitore da specifica normativa vigente. Entro i termini previsti, il Fornitore comunicherà all'Azienda l'avvenuta distruzione dei dati in proprio possesso ovvero le motivazioni per le quali non abbia provveduto all'operazione.

RIQUADRO 2. CLAUSOLA DA INSERIRE NEI CONTRATTI DI CONSULENZA

Nell'ambito delle attività previste dal contratto Lei è nominato Incaricato del trattamento dei dati, limitatamente alle seguenti tipologie di dati:

.....

Con la presente Lei si impegna ad effettuare il trattamento dei dati con competenza nel rispetto delle prescrizioni del DLgs 196/2003 e delle istruzioni specificate nelle seguenti Procedure Generali dell'Azienda:

PG 542.05 - Sicurezza dei dati e tutela della privacy

PG 63\_.13 - Modalità di utilizzo della rete Internet e delle caselle pubbliche di posta elettronica

PG 63\_.15 - Modalità di gestione delle credenziali di autenticazione e dei profili di autorizzazione per l'accesso ai dati mediante sistemi informatizzati.

Oltre a quanto specificato nelle predette PG dell'Azienda Lei dovrà attenersi alle seguenti ulteriori istruzioni:

.....

- e. Garantire, compatibilmente con le caratteristiche tecnologiche della procedura gestita, che sia possibile individuare "a posteriori" il codice di accesso che ha effettuato una data operazione sui dati contenuti nel data base della Procedura
- f. Definire le modalità di effettuazione delle operazioni di back up secondo le modalità operative identificate nella Procedura Generale PG 63\_.14.

L'Amministratore di procedura informatica centralizzata acquisita e gestita dalla SC Sistemi Informativi è nominato, su proposta del Direttore della SC Sistemi Informativi, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Direttore Generale mediante lettera di incarico (modulo MOD PG 542.05-12). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

L'Amministratore di procedura locale acquisita e gestita da una specifica SC è nominato, su proposta del Direttore della SC che gestisce la procedura locale, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Direttore Generale mediante lettera di incarico (modulo MOD PG 542.05-15). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti.

#### 6.3.8 AMMINISTRATORE DI PROCEDURA PER IL CONTROLLO OPERATIVO E IL MONITORAGGIO DELLE APPARECCHIATURE ELETTROMEDICALI/DISPOSITIVI MEDICI

Le funzioni e le responsabilità dell'Amministratore di Procedura per il controllo operativo e il monitoraggio delle apparecchiature elettromedicali/dispositivi medici sono:

- a. Conservare i codici e le password di accesso all'intera base dati della procedura e all'insieme completo delle funzionalità di elaborazione gestite dalla medesima
- b. Verificare periodicamente il rilascio di aggiornamenti firmware/software da parte del produttore dell'attrezzatura e provvedere alla loro installazione
- c. Compatibilmente con le caratteristiche tecnologiche della procedura e della strumentazione gestita, rilasciare i codici e le password da assegnare agli Incaricati dei trattamenti che utilizzano la procedura
- d. Definire le necessità e le modalità operative di effettuazione delle operazioni di backup.

L'Amministratore di procedura informatica per il controllo operativo e il monitoraggio delle apparecchiature elettromedicali/dispositivi medici è nominato, su proposta del Direttore della SC Tecnico, previo parere favorevole di Direttore Sanitario e Direttore Amministrativo, dal Direttore Generale mediante lettera di incarico (modulo MOD PG 542.05-15). Copia della lettera, controfirmata dall'interessato, viene conservata a cura del Responsabile della SS Affari Istituzionali nella raccolta dei documenti delle responsabilità e degli incarichi attribuiti

#### 6.3.9 RESPONSABILE DELLA SICUREZZA INFORMATICA DEGLI STRUMENTI (HW E SW) GESTITI CENTRALMENTE DALLA SC SISTEMI INFORMATIVI DELL'AZIENDA

Il Responsabile della sicurezza informatica degli strumenti Hw e Sw gestiti centralmente dalla SC Sistemi Informativi dell'Azienda è una persona con conoscenze informatiche adeguate a garantire la sicurezza informatica in Azienda. Ha la responsabilità di scegliere gli strumenti e le procedure più idonei a salvaguardare gli strumenti informatici centralizzati aziendali gestiti dalla SC Sistemi Informativi. Non rientrano tra le competenze della SC Sistemi Informativi la gestione e l'assistenza tecnica/manutenzione delle attrezzature e delle procedure informatiche locali e/o dipartimentali acquisite e gestite da una specifica SC e delle apparecchiature elettromedicali/dispositivi medici e relative procedure di controllo operativo e monitoraggio, secondo quanto individuato al punto § 6.3.4

Il Responsabile della sicurezza informatica degli strumenti (Hw e Sw) gestiti centralmente dalla SC Sistemi Informativi dell'Azienda è il Direttore della SC Sistemi Informativi.

#### 6.3.10 COMMISSIONE PRIVACY

La Commissione Privacy è una commissione permanente, nominata dal Direttore Generale con Deliberazione 428/DG/2004/SL del 21/05/2004, rinnovata e integrata con Deliberazioni 183/DG/2005/SL del 08/03/2005, 289/DG/2005/SL del 11/04/2005 e 176/DG/2008/DG del 03/04/2008, nella quale sono rappresentate tutte le Funzioni aziendali implicate nella definizione di misure adeguate al rispetto delle prescrizioni del Codice. La Commissione è composta da:

- ⊕ Il Direttore Sanitario dei Presidi
- ⊕ Il Rappresentante della Direzione
- ⊕ Il Direttore della SC Sistemi Informativi
- ⊕ Il Direttore della SC Tecnico e il responsabile dell'Ingegneria Clinica
- ⊕ Il titolare della Posizione Organizzativa per la sicurezza informatica degli strumenti centralizzati gestiti dalla SC Sistemi Informativi dell'Azienda
- ⊕ Il Responsabile della SS Affari Istituzionali
- ⊕ Il Responsabile della SS Legale
- ⊕ Il Responsabile dell'URP
- ⊕ Il Responsabile del SITRA.

Le funzioni della Commissione Privacy comprendono:

- a. Mantenere aggiornato l'elenco degli archivi cartacei e/o elettronici (centralizzati e non) dei dati personali e/o sensibili custoditi a livello aziendale, sulla base delle comunicazioni effettuate dai Responsabili del trattamento
- b. Mantenere aggiornato l'elenco dei trattamenti dei dati personali sensibili, sulla base delle comunicazioni effettuate dai Responsabili del trattamento
- c. Mantenere aggiornato il Documento Programmatico sulla Sicurezza dei dati
- d. Proporre al Direttore Generale misure strutturali, impiantistiche e strumentali di adeguamento dei percorsi aziendali alle norme sulla riservatezza
- e. Proporre al Direttore Generale piani per l'attività di formazione del personale in tema di normativa sulla riservatezza dei dati
- f. Promuovere attività per migliorare la consapevolezza sulla privacy in Azienda
- g. Analizzare le situazioni in cui si configuri un conflitto tra diritto alla riservatezza e dovere di garantire la trasparenza dell'attività amministrativa (vedi § 6.7.2)
- h. Vigilare sulla corretta attuazione delle decisioni assunte dal Direttore Generale in tema di tutela della privacy
- i. Assistere la Direzione nei rapporti con il Garante e con altri soggetti pubblici o privati rispetto agli adempimenti derivanti dalla normativa in materia.

#### 6.3.11 RESPONSABILITÀ DELLA SS AFFARI ISTITUZIONALI

La SS Affari Istituzionali è responsabile in Azienda della applicazione della normativa nazionale sulla Privacy e della gestione dei relativi adempimenti e procedimenti amministrativi necessari (notifiche al Garante della privacy, elenco dei trattamenti presenti in Azienda, nomina dei Responsabili del trattamento, deliberazioni inerenti i procedimenti amministrativi sulla Privacy, recepimento di regolamenti regionali, etc.)

### 6.4 Informativa e consenso al trattamento dei dati degli utenti

#### 6.4.1 INFORMATIVA

In tutti i luoghi dei Presidi dell'Azienda frequentati dagli utenti (DEA, ambulatori, reparti) viene esposta una informativa sulle modalità identificate dall'Azienda circa il trattamento dei dati personali (modulo MOD PG 542.05-01). Tale informativa è disponibile anche

presso l'Ufficio Relazioni con Il Pubblico (anche tradotta in diverse lingue), il Centro Unificato di Prenotazione, gli sportelli di prenotazione delle SC Radiologia e Laboratorio Analisi e presso gli operatori delle altre Strutture che effettuano attività di prenotazione non collegata con il CUP. L'informativa è disponibile anche sul sito Internet dell'Azienda (<http://www.cto.it>).

Per quanto riguarda le attività dell'Emergenza 118, quando possibile l'informativa viene fornita all'Interessato oralmente, specificando:

- ⊕ Che i dati personali vengono trattati per esclusiva finalità di cura, vengono trasmessi al personale del Pronto Soccorso di accoglienza e archiviati presso la Centrale Operativa 118, la sede della Associazione di Volontariato e/o la base Elisoccorso che hanno effettuato la missione
- ⊕ Che i dati personali non vengono comunicati a terzi
- ⊕ Quali sono i diritti relativamente al trattamento dei dati (vedi § 6.4.3)
- ⊕ Il nominativo del Responsabile del trattamento dei dati.

#### 6.4.2 ACQUISIZIONE DEL CONSENSO

Il consenso al trattamento dei dati viene acquisito con le modalità semplificate previste dagli articoli 78 e 81 del Codice. Gli operatori che effettuano la prenotazione delle prestazioni o la registrazione dei dati amministrativi al momento dell'accesso annotano sulla scheda anagrafica della procedura informatizzata la manifestazione del consenso. Tale informazione resta disponibile per tutti gli operatori coinvolti nel percorso del paziente, anche per accessi successivi alle Strutture dell'Azienda.

Nei casi in cui non sia possibile acquisire il consenso al trattamento dei dati con modalità semplificata (attività di prenotazione/accettazione non gestite con sistemi informatizzati) o allorché il paziente dichiara specifiche volontà circa la comunicazione dei suoi dati sensibili (vedi anche § 6.8.3) il consenso al trattamento dei dati viene acquisito in forma scritta utilizzando il modulo MOD PG 542.05-02. In questi casi i moduli compilati in occasione di ricovero vengono conservati all'interno della cartella clinica; per tutte le altre occorrenze i moduli compilati vengono conservati presso la Struttura che ha raccolto il consenso e sono allegati alla documentazione clinica.

Per quanto riguarda le attività dell'Emergenza 118, in base all'articolo 81, comma 2 del Codice, il consenso al trattamento dei dati è acquisito, quando possibile, oralmente dal personale in servizio sull'ambulanza e annotato sulla Scheda di ambulanza.

Nel caso in cui il paziente dichiara specifiche volontà circa la comunicazione dei suoi dati sensibili, il personale di ambulanza informa subito di ciò la Centrale Operativa, che provvede a registrare l'informazione sulla procedura informatizzata.

Nei casi in cui l'Interessato non sia in condizione di esprimere il proprio consenso, il consenso può essere acquisito per iscritto da un familiare o da un convivente, anche successivamente alla prestazione; se non è possibile raccogliere il consenso da parte di un familiare, sulla Scheda di ambulanza viene annotata l'impossibilità alla acquisizione del consenso (vedi anche § 6.8.4).

#### 6.4.3 DIRITTI DELL'INTERESSATO IN RELAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi del Codice ciascun Interessato ha diritto di:

- ⊕ Avere informazioni sull'esistenza o meno di propri dati personali in Azienda
- ⊕ Richiederne la modifica, il blocco del trattamento o la cancellazione, a meno che tali dati non siano gestiti o custoditi per obbligo di legge
- ⊕ Conoscere il nominativo dei Responsabili e/o degli Incaricati che trattano le sue informazioni.

#### 6.4.4 MODALITÀ DI ESERCIZIO DEI DIRITTI DA PARTE DELL'INTERESSATO

I diritti dell'Interessato possono essere fatti valere utilizzando i seguenti moduli:

- ⊕ MOD PG 542.05-03 - Esercizio del diritto ad essere informato sull'esistenza di dati personali in archivio e sul loro trattamento
- ⊕ MOD PG 542.05-04 - Esercizio del diritto ad ottenere rettifica o aggiornamento di dati presenti in archivio
- ⊕ MOD PG 542.05-05 - Esercizio del diritto ad ottenere cancellazione o blocco di dati presenti in archivio e trattati in violazione di legge
- ⊕ MOD PG 542.05-06 - Opposizione al trattamento dei dati per motivi legittimi.

I moduli compilati sono presentati all'URP, che avvia il procedimento avvalendosi della collaborazione del Responsabile del trattamento dei dati di competenza e interessando, ove necessario, la SS Affari Istituzionali, la SS Legale e il Consulente Medico-Legale dell'Azienda.

L'Interessato ha diritto ad ottenere risposta entro 30 giorni dalla data di ricevimento dell'istanza da parte dell'URP. La decorrenza di tale termine può essere bloccata solo in caso di necessità di ulteriori indagini o verifiche da parte dell'Azienda, la quale avrà cura di comunicare il blocco direttamente all'Interessato entro e non oltre 10 giorni dalla data di ricevimento dell'istanza. L'Interessato ha comunque diritto ad una risposta entro 60 giorni decorrenti dalla data di ricevimento dell'istanza.

L'Interessato, nell'esercizio dei diritti sopra riportati, può conferire per iscritto delega o procura a persone fisiche o ad Associazioni, mentre se tali diritti sono riferiti a dati personali concernenti persone decedute tali diritti possono essere esercitati da chiunque vi abbia un interesse giuridicamente rilevante, opportunamente documentato.

## 6.5 Informativa e consenso al trattamento dei dati dei dipendenti e dei fornitori

### 6.5.1 DIPENDENTI

All'atto della stipulazione del contratto individuale di lavoro, al dipendente neoassunto è consegnata copia dell'informativa (modulo MOD PG 542.05-07), resa a norma degli articoli 13 e 18 del Codice, relativa al trattamento operato dall'Azienda dei dati personali inerenti allo svolgimento del rapporto di lavoro e finalizzati in particolare all'instaurazione e alla gestione del rapporto medesimo attraverso l'adempimento di ogni obbligo contrattuale e legale ai fini della determinazione e del pagamento della retribuzione, dello sviluppo della posizione previdenziale ed assicurativa e di quanto altro conseguente il rapporto di lavoro.

Tale informativa precisa tra l'altro i diritti che, a proposito di tale trattamento, il dipendente può far valere nei confronti dell'Azienda a norma dell'articolo 7 del Codice, specificando nel contempo che l'esercizio di questi diritti non si estende alla creazione di dati non presenti negli archivi o alla loro rielaborazione personalizzata secondo criteri indicati dal dipendente medesimo (newsletter del Garante 13-19/10/2003 n. 187).

In ogni caso, trattandosi di Ente pubblico, ai sensi del combinato disposto dell'articolo 18 comma 4, dell'articolo 20 comma 1 e dell'articolo 112 del Codice, il trattamento dei dati sensibili attinenti allo svolgimento del rapporto di lavoro nei termini innanzi precisati non è subordinato al consenso dell'Interessato, purché ciò avvenga nel rispetto delle finalità di rilevante interesse pubblico individuate dalla legge nell'ambito del citato articolo 112 del Codice.

#### 6.5.2 FORNITORI

Relativamente al trattamento dei dati personali dei fornitori, nei capitolati di appalto stilati dalle Strutture afferenti al Dipartimento Tecnico Logistico viene inserita la clausola riportata nel Riquadro 3.

### 6.6 Misure strutturali per la protezione dei dati personali

Al di fuori degli orari di lavoro gli uffici e gli altri luoghi di lavoro (ad esempio gli ambulatori) in cui sono conservati documenti contenenti dati personali devono essere chiusi a chiave. Nei reparti di degenza la documentazione clinica dei pazienti ricoverati conservata nei locali ad uso medico che, per motivi di sicurezza, non possono essere chiusi a chiave, deve essere custodita (su scaffali o in carrelli) in modo tale che i dati dei pazienti non siano facilmente leggibili da parte di terzi.

Fuori dagli orari di servizio gli uffici e gli ambulatori sono accessibili solo da personale autorizzato, secondo criteri definiti da apposita Procedura aziendale. Le chiavi dei locali dell'Azienda sono custodite in portineria in modo tale che da esse non sia possibile risalire direttamente ai locali cui si riferiscono. Quando per qualsiasi motivo il personale autorizzato ritira in portineria una chiave firma un apposito registro, che riporta data e ora di prelievo e di restituzione della chiave. Le modalità di gestione delle chiavi di accesso ai locali dell'Azienda sono dettagliate alla Procedura Generale PG 64\_.04.

### 6.7 Misure organizzative generali per la protezione dei dati personali

#### 6.7.0 GENERALITÀ

I dati possono essere contenuti in atti e documenti cartacei presenti sulle scrivanie degli operatori, negli armadi, nei cassetti, su ripiani di appoggio, nei cestini dei rifiuti, oppure essere registrati su supporto magnetico ed essere contenuti quindi nelle memorie permanenti dei computer o dei server, nei floppy disk, nei CD-ROM o transitare attraverso le reti informatiche. Tali dati, se non custoditi con adeguate precauzioni, possono essere, anche involontariamente, divulgati all'esterno, consentendo a terze persone non autorizzate di conoscerli e trattarli.

Le tipologie di trattamenti che possono essere eseguiti sui dati personali sono elencate nella definizione fornita nel Glossario al § 6.1.2.

Tutto il personale dell'Azienda è tenuto a rispettare le istruzioni relative al trattamento dei dati riportate nei paragrafi seguenti del presente capitolo.

#### 6.7.1 CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto del diritto alla riservatezza e della dignità dell'Interessato.

Oggetto del trattamento devono essere i soli dati essenziali per svolgere attività istituzionali. I dati personali devono essere trattati in modo lecito, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni di trattamento in termini non incompatibili con tali scopi.

I dati eccedenti o non pertinenti alle finalità per le quali sono stati raccolti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I dati possono essere trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti.

RIQUADRO 3. CLAUSOLA DI RISERVATEZZA DA INSERIRE NEI CAPITOLATI DI APPALTO

**RISERVATEZZA DELLE INFORMAZIONI**

Per la presentazione dell'offerta, è richiesto ai concorrenti di fornire dati ed informazioni, anche sotto forma documentale, che rientrano nell'ambito di applicazione del decreto legislativo n. 196 del 30.6.2003.

Ai sensi e per gli effetti della citata normativa, all'Amministrazione aggiudicatrice compete l'obbligo di fornire alcune informazioni riguardanti il loro utilizzo.

Finalità del trattamento

In relazione alle finalità del trattamento dei dati forniti si precisa che:

- ⊕ I dati vengono acquisiti ai fini della partecipazione ed in particolare ai fini della effettuazione della verifica delle capacità amministrative e tecnico-economiche del concorrente all'esecuzione della fornitura, nonché dell'aggiudicazione e, per quanto riguarda la normativa antimafia, in adempimento di precisi obblighi di legge;
- ⊕ I dati da fornire da parte del concorrente aggiudicatario vengono acquisiti ai fini della stipula e dell'esecuzione del contratto, ivi compresi gli adempimenti contabili ed il pagamento del corrispettivo contrattuale.

Dati sensibili.

Di norma i dati forniti dai concorrenti e dall'aggiudicatario non rientrano tra i dati classificabili come "sensibili", ai sensi del decreto legislativo n. 196 del 30 giugno 2003.

Modalità del trattamento dei dati.

Il trattamento dei dati verrà effettuato in modo da garantire la sicurezza e la riservatezza e potrà essere attuato mediante strumenti manuali, informatici e telematici idonei a memorizzarli, gestirli e trasmetterli. Tali dati potranno essere anche abbinati a quelli di altri soggetti in base a criteri qualitativi, quantitativi e temporali di volta in volta individuati.

Categorie di soggetti ai quali i dati possono essere comunicati.

I dati potranno essere comunicati a:

- ⊕ Soggetti esterni, i cui nominativi sono a disposizione degli interessati, eventualmente facenti parte delle Commissioni di aggiudicazione che verranno di volta in volta costituite;
- ⊕ Regione Piemonte, relativamente ai dati forniti dal concorrente aggiudicatario;
- ⊕ Altri concorrenti che facciano richiesta di accesso ai documenti di gara nei limiti consentiti ai sensi della Legge n. 241/1990.

Diritti del concorrente interessato

Relativamente ai suddetti dati, al concorrente, in qualità di interessato, vengono riconosciuti i diritti di cui al citato decreto.

Acquisite le suddette informazioni, ai sensi del decreto 196/2003 con la presentazione dell'offerta, il concorrente acconsente espressamente al trattamento dei dati personali secondo le modalità indicate precedentemente.

Il concorrente potrà specificare se e quale parte della documentazione presentata, ritiene coperta da riservatezza, con riferimento a marchi, know-how, brevetti ecc.: in tal caso l'Amministrazione aggiudicatrice non consentirà l'accesso a tale documentazione in caso di richiesta di altri concorrenti.

I trattamenti dei dati devono essere effettuati nel pieno rispetto delle misure minime di sicurezza riportate ai paragrafi successivi e nel DPS per quanto riguarda i dati trattati con strumenti elettronici, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Qualora i provvedimenti da pubblicare contengano dati sensibili, l'Azienda seleziona, alla luce dei principi di pertinenza e non eccedenza, i dati personali la cui inclusione nei provvedimenti da pubblicare sia realmente necessaria per le finalità proprie di ciascuno di questi.

#### 6.7.2 RAPPORTI TRA DIRITTO DI ACCESSO E DIRITTO ALLA RISERVATEZZA

In osservanza degli articoli 59 e 60 del Codice, che in tema di dati personali fa esplicitamente salve le vigenti norme in materia di accesso ai documenti amministrativi, il Responsabile del trattamento dei dati valuta caso per caso, con il supporto della SS Legale e del Consulente Medico-Legale dell'Azienda la possibilità di accedere ai documenti da parte di terzi. L'accesso sarà ammesso sulla base delle indicazioni fornite dalla Procedura Generale PG 42\_.01.

L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali contenuti in documenti amministrativi è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango pari almeno al diritto alla riservatezza, ovvero consiste in un diritto alla personalità o in altro diritto o libertà fondamentale o inviolabile, quale ad esempio il diritto alla difesa.

#### 6.7.3 ISTRUZIONI GENERALI PER GLI INCARICATI DEL TRATTAMENTO DEI DATI

L'accesso agli archivi dell'Azienda è autorizzato solo al Titolare e alle persone che abbiano ricevuto formale lettera di incarico per il trattamento dei dati o per le quali, usufruendo della modalità semplificata di incarico, vi sia evidenza della presa visione del documento che definisce l'ambito di trattamento previsto all'interno della struttura di appartenenza (vedi § 6.3.3).

Per impedire a persone non autorizzate di accedere a documenti o informazioni contenenti dati personali i documenti amministrativi e la documentazione clinica relativa ai pazienti (cartelle cliniche, registri operatori, registri nosologici, consegne e schede infermieristiche, schede di dimissione, registri degli stupefacenti, referti, etc.) non devono essere lasciati su tavoli, desk o scaffali in condizioni tali da permetterne la lettura da parte di estranei, ma conservati in luoghi non accessibili a terzi non autorizzati e/o con modalità tali da non renderne agevole la lettura (archivi, classificatori). Floppy disk e CD-ROM devono essere conservati in cassette o contenitori e non lasciati sul tavolo di lavoro.

I documenti contenenti dati personali che vengono prelevati da archivi per l'attività quotidiana devono essere riposti a fine giornata.

I documenti elettronici contenenti dati personali non devono essere archiviati sul *desktop* del computer, ma in *directory* del disco rigido o del file server.

Le copie cartacee o elettroniche di documenti contenenti dati personali eseguite per motivo di servizio devono essere distrutte quando il loro utilizzo non è più necessario.

Quando ci si allontana dalla postazione di lavoro informatizzata occorre disconnettersi o, quanto meno, attivare lo *screen saver* che, dopo un certo periodo di inattività del computer, richiede nuovamente la password per accedere ai dati. A fine lavoro gli archivi elettronici devono essere chiusi e i computer devono essere spenti o, quanto meno, deve essere chiusa la sessione di lavoro.

Ogni messaggio di posta elettronica inviato attraverso un account del dominio cto.to.it deve riportare in calce la clausola riportata nel Riquadro 4.

Le istruzioni per inserire la clausola nei messaggi di posta elettronica sono riportate sul sito Intranet dell'Azienda.

Alla stessa stregua i fax inviati dall'interno dell'Azienda devono riportare in calce la clausola riportata nel Riquadro 5.

RIQUADRO 4. CLAUSOLA DA RIPORTARE IN CALCE AI MESSAGGI DI POSTA ELETTRONICA

Le informazioni contenute in questa comunicazione e gli eventuali documenti allegati hanno carattere confidenziale e sono a uso esclusivo del destinatario. Nel caso questa comunicazione Vi sia pervenuta per errore, Vi informiamo che la sua diffusione e riproduzione è contraria alla legge, Vi preghiamo di darci prontamente avviso e di cancellare quanto ricevuto. Grazie.

This e-mail message and any files transmitted with it contain confidential information intended only for the person(s) to whom it is addressed. If you are not the intended recipient, you are hereby notified that any use or distribution of this e-mail is strictly prohibited: please notify the sender and delete the original message. Thank you.

RIQUADRO 5. CLAUSOLA DA RIPORTARE IN CALCE AI FAX

Il presente fax potrebbe contenere informazioni da considerarsi strettamente riservate ad esclusivo utilizzo del destinatario in indirizzo, che è l'unico autorizzato ad usarlo, copiarlo e, sotto la propria responsabilità, diffonderlo. Chiunque dovesse ricevere questo fax per errore o comunque lo leggesse senza esserne legittimato è avvertito che trattenerlo, copiarlo, divulgarlo e distribuirlo a persone diverse dal destinatario è proibito dalla legge italiana. Egli è pregato di avvertire immediatamente il mittente e di distruggerlo.

## 6.8 Istruzioni specifiche relative al trattamento dei dati sensibili

### 6.8.1 PRESENZA DEI PAZIENTI IN OSPEDALE

Salvo diversa manifestazione di volontà è consentito comunicare a terzi legittimati (esercenti la potestà legale, prossimi congiunti o familiari) la presenza degli Interessati presso reparti dell'Azienda.

Nel caso in cui, al momento del ricovero, un paziente esprima la volontà che non venga comunicata la sua presenza in ospedale è possibile selezionare sulla maschera di accettazione della procedura informatizzata l'opzione "Episodio anonimo". In tal modo nell'elenco dei pazienti ricoverati che è disponibile a video agli operatori di Portineria, Ufficio Informazioni e URP non compare il nominativo del paziente che ha espresso tale volontà.

### 6.8.2 IDENTIFICAZIONE DEI DEGENTI IN REPARTO

Generalmente nell'ufficio del Coordinatore Infermieristico dei reparti i dati identificativi dei pazienti ricoverati (e a volte anche informazioni utili per le consegne) sono riportati su tabelloni appesi ad un muro. Tali tabelloni devono essere sistemati in modo tale che le informazioni non siano leggibili dalla porta di accesso al locale.

I fogli di diaria, che riportano le rilevazioni dei parametri vitali dei pazienti (temperatura, pressione arteriosa, diuresi, etc.) devono essere conservati all'interno della cartella clinica oppure custoditi nella stanza di degenza all'interno di una cartellina o in modo che le informazioni sanitarie non siano leggibili da parte di persone terze.

### 6.8.3 MODALITÀ DI INFORMAZIONE DEI PAZIENTI E DEI TERZI LEGITTIMATI

In base all'articolo 84 del Codice la comunicazione di dati personali idonei a rivelare lo stato di salute all'interessato o a terzi legittimati (esercenti la potestà legale, prossimi congiunti o familiari) può essere fornita solo da un medico designato dall'Interessato o dal Titolare.

Qualora singoli Responsabili intendano designare altro personale sanitario a fornire informazioni, tale trattamento dovrà essere evidenziato nella lettera di incarico (vedi § 6.3.3) e dovranno essere anche fornite specifiche istruzioni sulle modalità e cautele che dovranno da questi essere adottate nella comunicazione.

Prima di dare informazioni a terzi legittimati occorre comunque verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione e accertarsi, per quanto ragionevole, dell'identità dei soggetti richiedenti (i terzi legittimati sono rappresentati da genitori, fratelli, figli, coniugi o conviventi, nonni e nipoti, e da chi dimostra di avere la potestà legale sull'Interessato).

Tutti gli operatori sono tenuti ad evitare di discutere sulle condizioni cliniche dei pazienti pubblicamente o in presenza di persone "non addette ai lavori", facendo espliciti riferimenti che rendano identificabile la persona.

E' fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'Addetto Stampa.

#### 6.8.4 INFORMAZIONI DA PARTE DEL SISTEMA EMERGENZA 118

L'evenienza che possa essere data informazione, anche telefonica, a terzi legittimati di prestazioni di pronto soccorso è espressamente prevista dal Codice (articolo 83, comma 2, lettera f) e confermata dal Provvedimento del Garante 09/11/2005 (documento web 1191411), a patto che siano rispettate alcune condizioni.

Sulla base delle previsioni normative sopra citate il Titolare del trattamento dei dati autorizza per iscritto il personale sanitario del Sistema Emergenza 118 a rendere noti dati personali idonei a rilevare lo stato di salute di persone oggetto di una prestazione di pronto soccorso solo a terzi legittimati (esercenti la potestà legale, prossimi congiunti o familiari) anche per via telefonica, sulla base delle seguenti istruzioni specifiche:

- ⊕ Prima di dare informazioni il personale di Centrale deve assicurarsi che sul sistema informativo non siano registrate indicazioni contrarie da parte dell'interessato
- ⊕ Se non sono state espresse indicazioni contrarie da parte dell'interessato (o se l'interessato non è stato in condizione di esprimere il consenso), prima di dare le informazioni il personale che opera in Centrale deve assicurarsi, per quanto ragionevolmente possibile, del rapporto di parentela che intercorre fra chi richiede le informazioni e l'interessato, rammentando al richiedente, se del caso, che la conversazione è registrata e che le conseguenze di eventuali false dichiarazioni potranno essere perseguite (articolo 167 del Codice)
- ⊕ Le informazioni potranno essere rilasciate solo a richiedenti quali genitori, fratelli, figli, coniugi o conviventi, nonni e nipoti, oltre che a chi dichiara di avere la potestà legale sull'interessato
- ⊕ Prima di ricevere le informazioni il richiedente dovrà dichiarare in modo chiaro e comprensibile il proprio nominativo e l'indirizzo di residenza
- ⊕ Solo in questo caso, e se non sussistono indicazioni contrarie da parte dell'interessato, l'operatore potrà fornire le informazioni strettamente necessarie a confermare o meno che l'interessato sia stato soccorso dal 118 e, nel caso l'intervento sia stato effettuato, l'ospedale presso cui l'interessato è stato trasportato
- ⊕ Non dovranno comunque essere rilasciate informazioni sul luogo di effettuazione dell'intervento, né sullo stato di salute dell'interessato.

#### 6.8.5 DOCUMENTI SANITARI GENERATI DURANTE L'EROGAZIONE DELLE PRESTAZIONI

Le modalità di gestione delle Cartelle Cliniche di ricovero e ambulatoriali sono dettagliate nella Procedura Generale PG 424.03. Nell'ambito della citata Procedura vengono date anche indicazioni relative alle modalità di trattamento dei dati sanitari in esse contenuti.

La documentazione clinica (richieste, esami di laboratorio, referti, note operatorie, cartelle cliniche) dei pazienti ricoverati deve essere movimentata nell'ambito dei Presidi e tra i Presidi dell'Azienda utilizzando buste o classificatori, in modo da non permettere l'identificazione del paziente e la lettura dei dati sensibili. Il recapito e la gestione delle ri-

chieste di consulenza (prima e dopo la loro effettuazione) devono essere effettuati in modo da non permettere a terzi l'identificazione del paziente.

Qualsiasi documento relativo ad attività sanitarie (referti di esami di laboratorio, referti di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusa direttamente all'Interessato. Il ritiro della documentazione sanitaria è ammesso anche da parte di persona delegata per iscritto dall'Interessato.

Le modalità di gestione delle ricette mediche sono dettagliate nella Procedura Generale PG 424.04.

Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati devono essere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardanti lo stato di salute della persona interessata.

#### 6.8.6 DOCUMENTI DI PROPRIETÀ DEI PAZIENTI

I documenti portati in visione dal paziente devono essere conservati rispettando le regole di tutela del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente in busta chiusa.

### 6.9 Misure per la protezione dei dati trattati con l'ausilio di strumenti elettronici

#### 6.9.1 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Le misure adottate dall'Azienda per la protezione dei dati trattati con l'ausilio di strumenti elettronici, nonché la pianificazione degli interventi previsti per migliorare nel tempo le misure minime adottate sono contenute nel Documento Programmatico sulla Sicurezza (DPS), redatto a norma dell'articolo 34 e della regola 19 dell'Allegato B del Codice.

Come previsto dalla regola 19 dell'Allegato B del Codice, il DPS viene aggiornato entro il 31 Marzo di ogni anno; tale aggiornamento è effettuato a cura della SS Affari Istituzionali (vedi § 6.3.11) con il supporto di tutta la Commissione Privacy (vedi § 6.3.10).

#### 6.9.2 MONITORAGGIO DELLA POSTA ELETTRONICA E DEGLI ACCESSI AD INTERNET

Al controllo della posta elettronica e degli accessi ad Internet da parte degli operatori dell'Azienda è applicato il principio di proporzionalità e non eccedenza e deve tenere conto della legittima Privacy e di altri interessi del dipendente.

I dati sono raccolti per scopi specifici, espliciti e legittimi e non utilizzati in modo illecito. I dati non indispensabili o eccedenti gli scopi per i quali il monitoraggio viene effettuato devono essere distrutti, salvo diversa disposizione dell'Autorità Giudiziaria.

I dati raccolti a seguito del monitoraggio della posta elettronica e degli accessi ad Internet da parte degli operatori dell'Azienda devono essere esatti ed aggiornati. Il lavoratore ha il diritto di rettifica ed integrazione delle informazioni. Il lavoratore è adeguatamente informato sulla possibilità che vengano effettuati controlli.

Le attività inerenti sono specificate nella Procedura Generale PG 63\_.13.

#### 6.9.3 MONITORAGGIO DEL TRAFFICO TELEFONICO

Relativamente alle informazioni sul traffico telefonico generato/ricevuto dall'Azienda, la Tabella 2 riporta i trattamenti effettuati.

TABELLA 2. TRATTAMENTI EFFETTUATI SUL TRAFFICO TELEFONICO

Tipologia	Monitoraggio
Centralino Aziendale	Dal 01/05/2003 vengono archiviate le informazioni sul traffico entrante/uscente dal centralino dei Presidi CTO, CRF e Maria Adelaide con specifica di numero chiamato, numero chiamante e durata della conversazione. Le chiamate a cui non corrisponde una risposta, sia in entrata che in uscita, non sono archiviate.
Centralino 118	Le conversazioni sono registrate su supporto custodito presso locali protetti della centrale operativa secondo le modalità descritte nel DPS Aziendale.
Linee dedicate	L'Azienda non monitorizza il traffico delle linee dedicate. Eventuali informazioni sul traffico generato sono quelle descritte dal fornitore all'atto di emissione della fattura
Telefonia Mobile Aziendale	L'Azienda non monitorizza il traffico. All'atto dell'emissione della fattura il fornitore fornisce per ogni utenza e per ogni chiamata il numero chiamato (oscurato delle ultime 3 cifre) e la durata della conversazione.

## 6.10 Misure strutturali e organizzative per tutelare la riservatezza degli utenti

### 6.10.1 ATTESA E CHIAMATA PER PRESTAZIONI

La chiamata per la visita dei pazienti in attesa presso le aree ambulatoriali avviene utilizzando un codice alfanumerico anonimo consegnato al paziente al momento della accettazione. Dove possibile viene utilizzato un unico codice per la chiamata a diverse prestazioni eseguite nell'ambito del percorso previsto dello stesso accesso.

### 6.10.2 DISTANZA DI CORTESIA AGLI SPORTELLI

Agli sportelli di prenotazione e accoglienza è assicurata la distanza di cortesia, segnalata da una striscia autoadesiva di colore rosso sul pavimento.

### 6.10.3 RISERVATEZZA DEI COLLOQUI

Tutto il Personale è invitato ad assicurare la massima riservatezza nei colloqui con i pazienti. A tale scopo vengono suggerite le seguenti raccomandazioni:

- ⊕ Nella raccolta dell'anamnesi o quando è necessario comunicare ai pazienti ricoverati notizie riguardanti il loro stato di salute si raccomanda di adottare comportamenti che riducano la possibilità di divulgazione di informazioni a terzi (ad esempio effettuando i colloqui in locali dedicati, oppure chiedendo ai parenti di uscire dalla stanza, pregando gli altri pazienti ricoverati, quando possibile, di accomodarsi nel soggiorno, accostandosi quanto più possibile al letto del paziente, moderando il volume della voce)
- ⊕ Durante le visite ambulatoriali si raccomanda di evitare l'accesso alla stanza di visita da parte di persone non coinvolte e di moderare il volume della voce per non permettere l'ascolto da parte di persone che sostano in corridoio.

### 6.10.4 IMPIANTI DI VIDEO-SORVEGLIANZA

Agli impianti di video-sorveglianza installati nell'ambito dell'Azienda e, in particolare, al trattamento dei dati raccolti con tali attrezzature, è applicato il principio di proporzionalità tra mezzi impiegati e fini perseguiti. Le modalità operative di gestione degli impianti di video-sorveglianza e le modalità di trattamento dei dati relativi sono contenute nella Procedura Generale PG 63\_.16, sulla base dei seguenti requisiti:

- ⊕ Ogni installazione deve essere autorizzata dal Direttore Generale
- ⊕ Il trattamento dei dati raccolti tramite video-sorveglianza deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi e deve rispettare i principi di pertinenza e non eccedenza
- ⊕ I dati acquisiti tramite tali impianti possono essere trattati esclusivamente da parte di Incaricati del trattamento autorizzati con specifico e formale atto di nomina.

Rimane ferma la disciplina di tutela del lavoratore dipendente di cui alla Legge 300/1970 per quanto riguarda il divieto del controllo del lavoratore a distanza.

## 6.11 Politica per la Privacy

Sul sito Internet dell'Azienda (<http://www.cto.to.it>) è pubblicata, la Politica per la Privacy definita dal Direttore Generale.

## 6.12 Rapporti con il Garante

Ogni rapporto col Garante è di competenza del Titolare, il quale vi provvede con il supporto della SS Affari Istituzionali e della Commissione Privacy.

In particolare il Titolare procede a nuova notificazione dei trattamenti di dati personali svolti nell'ambito dell'Azienda ove muti taluno degli elementi indicati all'articolo 37 del Codice ed effettua le comunicazioni previste dall'articolo 39.

## 7. DOCUMENTI E REGISTRAZIONI CORRELATI

### Normativa

- ⊕ DPR 10/01/1957 n. 3 - Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato, articolo 15
- ⊕ Legge 20/05/1970 n. 300 - Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento
- ⊕ DLgs 30/06/2003 n. 196 - Codice in materia di protezione dei dati personali
- ⊕ Deliberazione del Garante 23/12/2004 n. 14 - Contributo spese relativo all'esercizio dei diritti di accesso dell'interessato
- ⊕ Provvedimento del Garante 09/11/2005 (documento web 1191411)
- ⊕ DPGR Regione Piemonte 3/R del 11/05/2006 - Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione
- ⊕ DPGR Regione Piemonte 14/R del 04/12/2006 - Rettifica dell'allegato B del DPGR 3/R del 11/05/2006.

### Deliberazioni del Direttore Generale

- ⊕ Deliberazione 441/C/98/UAI del 18/03/1998 - Nomina degli Incaricati del trattamento dei dati personali
- ⊕ Deliberazione 428/DG/2004/SL del 21/05/2004 - Nomina della Commissione per gli adempimenti attuativi del Codice
- ⊕ Deliberazione 516/DG/2004/UAI del 30/06/2004 - Nomina dei Responsabili del trattamento dei dati personali
- ⊕ Deliberazione 183/DG/2005/SL del 08/03/2005 - Sostituzione ed integrazione dei componenti della Commissione Privacy
- ⊕ Deliberazione 289/DG/2005/SL del 11/04/2005 - Ulteriore integrazione dei componenti della Commissione Privacy
- ⊕ Deliberazione 719/DG/2005/UAI del 21/10/2005 - Sicurezza dei dati e tutela della privacy. Approvazione Procedura Generale PG 542.05 e nomina dei Responsabili del trattamento dei dati
- ⊕ Deliberazione 176/DG/2008/DG del 03/04/2008 - Sicurezza dei dati e tutela della privacy - Approvazione revisione della procedura generale PG 542.05 e rinnovo dei componenti della Commissione privacy

### Documenti generali del SGQ aziendale applicabili

- ⊕ Manuale Aziendale del SGQ (capitolo 5)
- ⊕ DPS - Documento Programmatico sulla Sicurezza

### Procedure Generali

- ⊕ Procedura Generale PG 42\_.01 - Accesso ai documenti
- ⊕ Procedura Generale PG 424.03 - Gestione della cartella clinica
- ⊕ Procedura Generale PG 424.04 - Gestione delle ricette mediche

- ⊕ Procedura Generale PG 63\_.13 - Modalità di utilizzo della rete Internet e delle caselle pubbliche di posta elettronica
- ⊕ Procedura Generale PG 63\_.14 - Modalità di gestione dei backup dei dati trattati con sistemi informatici e del ripristino dei sistemi in caso di malfunzionamenti
- ⊕ Procedura Generale PG 63\_.15 - Modalità di gestione delle credenziali di autenticazione e dei profili di autorizzazione per l'accesso ai dati mediante sistemi informatizzati
- ⊕ Procedura Generale PG 63\_.16 - Gestione degli impianti di video-sorveglianza
- ⊕ Procedura Generale PG 64\_.04 - Modalità di gestione delle chiavi di accesso ai locali dell'Azienda

#### Moduli

- ⊕ Modulo MOD PG 542.05-01 - Informativa ai clienti
- ⊕ Modulo MOD PG 542.05-02 - Acquisizione del consenso per il trattamento dei dati sensibili
- ⊕ Modulo MOD PG 542.05-03 - Esercizio del diritto di essere informato sull'esistenza di dati personali in archivio e sul loro trattamento
- ⊕ Modulo MOD PG 542.05-04 - Esercizio del diritto di ottenere rettifica o aggiornamento di dati presenti in archivio
- ⊕ Modulo MOD PG 542.05-05 - Esercizio del diritto di ottenere cancellazione o blocco di dati presenti in archivio e trattati in violazione di legge
- ⊕ Modulo MOD PG 542.05-06 - Opposizione al trattamento dei dati per motivi legittimi
- ⊕ Modulo MOD PG 542.05-07 - Informativa al dipendente neo assunto sul trattamento dei dati personali attinenti il rapporto di lavoro
- ⊕ Modulo MOD PG 542.05-10 - Lettera di incarico per Amministratore di Rete
- ⊕ Modulo MOD PG 542.05-11 - Lettera di incarico per Amministratore di Server
- ⊕ Modulo MOD PG 542.05-12 - Lettera di incarico per Amministratore di Procedura
- ⊕ Modulo MOD PG 542.05-15 - Lettera di incarico per Amministratore di Procedura locale
- ⊕ Modulo MOD PG 542.05-13 - Lettera di incarico per Responsabile del trattamento dei dati
- ⊕ Modulo MOD PG 542.05-14 - Lettera di incarico per Incaricato del trattamento dei dati

#### Registrazioni

- ⊕ Archivio delle lettere di incarico a Responsabile del trattamento dei dati e ad Amministratore di sistema, gestito dal Responsabile della SS Affari Istituzionali
- ⊕ Archivi delle lettere di incarico a Incaricato del trattamento dei dati, gestiti dai singoli Responsabili del trattamento dei dati.

### **8. ELENCO DI DISTRIBUZIONE**

- ⊕ Direttore Generale
- ⊕ Direttore Amministrativo
- ⊕ Direttore Sanitario
- ⊕ Direttore Sanitario dei Presidi
- ⊕ Direttori dei Dipartimenti
- ⊕ Direttori di Strutture Complesse
- ⊕ Responsabile del SITRA
- ⊕ Responsabile del Servizio Prevenzione e Protezione
- ⊕ Responsabile dell'Ufficio Relazioni con il Pubblico
- ⊕ Responsabile della Carta dei Servizi.

### **9. DIFFUSIONE**

Il testo del presente Documento è messo a disposizione di tutto il Personale dell'Azienda mediante inserimento nell'apposita sezione dell'Intranet Aziendale.