

<p>ASL Roma B</p>	<p>STAFF DIREZIONE AZIENDALE UNITA' OPERATIVA COMPLESSA "QUALITA' AZIENDALE E PROGETTO COMUNICAZIONE, RISK MANAGEMENT, PRIVACY" DIRETTORE: DR. EGIDIO SESTI</p>	<p>Revisione n. 0 Revisione programmata: 1 aprile 2007</p>	<p>Codice Documento Py 2 - 06 Pagina 1 di 13</p>
------------------------------	---	---	---

PROCEDURE PRIVACY PER INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

**Cod. Doc.
Py 2 - 06**

Data redazione	Redazione	Verifica	Firma
Marzo 2006	Dott. Egidio Sesti (Referente Aziendale Privacy) Componenti Gruppo Privacy D.ssa Anna Ascione Dott. Fausto Bandiera Dr. Pierfrancesco Calzetta Sig. Salvatore Manfredi Avv. Massimo Micheli Dott. Alfredo Pietroletti Avv. Mauro Alicandro Dott. Giuseppe Scarola	Dott. Bruno Cinque	
Firma			
	Approvazione	Approvazione	Approvazione
	Direttore Generale Dott.ssa Flori Degrassi	Direttore Sanitario Dott. Antonio D'Urso	Direttore Amministrativo Dott. Alessandro Cipolla
Firma			

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 3 di 13
PROCEDURE PRIVACY PER INCARICATI				

INDICE

<u>AMBITO</u>	<u>4</u>
<u>SCOPO E CAMPO DI APPLICAZIONE</u>	<u>4</u>
<u>DOCUMENTI DI RIFERIMENTO</u>	<u>4</u>
<u>DEFINIZIONI</u>	<u>5</u>
<u>ISTRUZIONE PER LE CREDENZIALI DI AUTENTICAZIONE</u>	<u>7</u>
1. PASSWORD INIZIALE	7
2. LUNGHEZZA DELLA PASSWORD	7
3. SCELTA E COSTRUZIONE DELLA PASSWORD	7
4. RISERVATEZZA DELLA PASSWORD	8
5. AGGIORNAMENTO DELLA PASSWORD	8
<u>ISTRUZIONI PER UTILIZZO PC</u>	<u>9</u>
<u>ISTRUZIONI PER LA GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI</u>	<u>9</u>
<u>ISTRUZIONI PER IL TRATTAMENTO DEI DOCUMENTI CARTACEI</u>	<u>10</u>
1. ARCHIVIAZIONE DEI DOCUMENTI CARTACEI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
2. CONSULTAZIONE DEI DOCUMENTI CARTACEI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
3. CONSEGNA DEI DATI AGLI INTERESSATI - INCARICATI	12
4. DISTRUZIONE DEI DOCUMENTI CARTACEI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
<u>ALLEGATO 1</u>	<u>13</u>

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 4 di 13
PROCEDURE PRIVACY PER INCARICATI				

AMBITO

Il presente documento si inquadra nell'ambito delle Misure Minime di Sicurezza, previste dall'allegato B del Decreto Legislativo n. 196 del 30 Giugno 2003, applicabili alla Azienda ASL Roma B.

SCOPO E CAMPO DI APPLICAZIONE

Il presente documento, strutturato in differenti sezioni, ha l'obiettivo di specificare le istruzioni operative a cui si devono attenere gli Incaricati al trattamento dei dati personali della Azienda ASL Roma B, in conformità con la Normativa vigente in materia di trattamento dei Dati Personali, Sensibili e Giudiziari (Decreto Legislativo n. 196 del 30 giugno 2003).

Si precisa comunque che possono essere eseguite attività in autonomia purché non comportino una diminuzione del livello generale e specifico di sicurezza.

I soggetti incaricati a trattare i dati personali (cioè tutti quei dati idonei ad identificare direttamente o indirettamente una persona fisica o giuridica, come i dati anagrafici, i recapiti telefonici, gli indirizzi, i dati sullo stato di salute, ecc.), si atterranno alle seguenti modalità ed istruzioni:

L'Azienda ASL Roma B, tramite verifiche periodiche, direttamente o con l'ausilio di altre società, effettuerà i controlli che riterrà opportuni per vigilare sulla puntuale osservanza delle disposizioni della normativa vigente e delle presenti Istruzioni Operative.

DOCUMENTI DI RIFERIMENTO

Decreto Legislativo n. 196 del 30 giugno 2003.

DPS - Azienda ASL Roma B

Procedura informatica

Regolamento aziendale sulla Privacy (cod. doc. Py 1 – 06) ed in particolare **l'art. 5**

I documenti disponibili in formato elettronico sono pubblicati sull'area Intranet della Azienda ASL Roma B.

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 5 di 13
PROCEDURE PRIVACY PER INCARICATI				

Istruzioni generali

- il trattamento deve essere effettuato in modo lecito, secondo correttezza e, comunque, in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza;
- i dati devono essere raccolti e registrati solo per gli scopi inerenti l'attività svolta dall'Unità;
- deve essere, ove possibile, verificata l'esattezza dei dati e ne deve essere effettuato l'aggiornamento;
- deve essere verificato che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono state raccolti o successivamente trattati;
- i dati sensibili, contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi, che permettano di identificare gli interessati solo in caso di necessità;
- i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo;
- i dati devono essere conservati rispettando le misure di sicurezza, individuate nel documento programmatico sulla sicurezza elaborato dall'azienda ed in particolare le linee-guida per dare piena applicazione alle misure minime di sicurezza di cui al D.P.R. 28 luglio 1999, n. 318, previste dal regolamento aziendale attuativo della legge 675/1996;
- nessun dato può essere comunicato a terzi o diffuso senza la preventiva specifica autorizzazione dello scrivente;
- in caso di allontanamento dal posto di lavoro, l'incaricato deve adottare le misure in atto e a sua disposizione, secondo le istruzioni ricevute, per evitare l'accesso ai dati personali trattati o in trattamento, sia cartaceo che automatizzato, da parte di terzi, anche se dipendenti a meno che non siano autorizzati.

DEFINIZIONI

Ai fini del presente documento, si applicano, le definizioni riportate nel Codice in materia di protezione dei dati personali quali:

Tabella 1: Definizioni

Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità
Banca di 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	I dati ed i dispositivi, in possesso di una persona, da questa

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06	Pagina 6 di 13
PROCEDURE PRIVACY PER INCARICATI			
Dato anonimo	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.		
Dato giudiziario	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.		
Dato identificativo	Dato personale che permette l'identificazione diretta dell'interessato.		
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.		
Dato personale pubblico	Dato personale di dominio pubblico (es. rubriche telefoniche pubbliche)		
Dato sensibile	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.		
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.		
Garante per la protezione dei dati personali	L'autorità di cui all'articolo n. 153 del D.Lgs. n. 196., istituita dalla legge 31 dicembre 1996, n. 675		
Incaricato	Le persone fisiche autorizzate a compiere operazioni di <i>trattamento</i> dal titolare o dal responsabile.		
Interessato	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.		
Misure minime	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.		
Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica		
Responsabile del trattamento	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.		
Strumenti elettronici	Gli elaboratori, i 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 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.		

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06	Pagina 7 di 13
PROCEDURE PRIVACY PER INCARICATI			
Trattamento	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.		

ISTRUZIONE PER LE CREDENZIALI DI AUTENTICAZIONE

Lo scopo di questa sezione è di fornire le Istruzioni Operative riguardanti il processo di autenticazione, in particolare per l'utilizzo della password.

Il processo di autenticazione descritto in questa sezione prevede l'inserimento di un codice identificativo dell'Utente (Incaricato) associato a una parola chiave riservata (password) .

Password iniziale

- La prima password viene comunicata in modalità riservata all'Incaricato, con comunicazione che invita ad effettuare immediatamente la sostituzione.
- La prima password ha carattere provvisorio; non attiva alcuna operazione diversa da quelle strettamente necessarie alla sua sostituzione da parte dell'Incaricato.
- L'utente non deve effettuare alcuna operazione se prima non ha provveduto a sostituire la password iniziale.
- L'incaricato effettua la sostituzione della prima password attenendosi alle raccomandazioni fornite nell'Allegato 1.

Lunghezza della password

La lunghezza minima della password deve essere almeno di otto caratteri. Nel caso in cui il sistema non consenta l'utilizzo di una password di 8 caratteri, deve essere utilizzato un numero di caratteri pari al massimo consentito .

Scelta e costruzione della password

La password scelta non deve essere banale o facilmente individuabile pertanto è necessario

attenersi alle raccomandazioni fornite nell'Allegato 1.

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 8 di 13
PROCEDURE PRIVACY PER INCARICATI				

Riservatezza della password

Occorre adottare le necessarie cautele per assicurare la segretezza e la riservatezza della password.

L'Incaricato al trattamento è tenuto alla custodia della password attenendosi alle seguenti disposizioni:

- La password di accesso relativa ad un Incaricato è strettamente personale e non può essere comunicata ad altri;
- Non è consentita la trascrizione della password su carta o su qualsiasi altro supporto;
- L'Incaricato non deve lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- La perdita o la diffusione di una password personale deve prontamente essere comunicata al Titolare/Responsabile del Trattamento e al Responsabile I.T. .

Aggiornamento della password

L'aggiornamento della password è consentito esclusivamente all'Incaricato attenendosi alle seguenti disposizioni:

la password deve essere aggiornata dall'Incaricato al primo utilizzo e successivamente almeno ogni tre mesi;

dove tecnicamente possibile deve essere concessa all'Utente finale la possibilità di sostituire in qualsiasi momento ed autonomamente le password di accesso alle informazioni in caso di sospetto di compromissione della riservatezza.

L'Incaricato aggiorna la propria password personale, avvalendosi delle regole fornite in Allegato 1, al verificarsi di uno dei seguenti eventi:

immediatamente in caso di prima attivazione;

per decorrenza del periodo di validità attribuito alla password 3 mesi;

su esplicita richiesta del Responsabile I.T. .

E' vietata la sostituzione di una password con una frequenza superiore alle 2 volte al giorno.

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 9 di 13
PROCEDURE PRIVACY PER INCARICATI				

ISTRUZIONI PER UTILIZZO PC

Lo scopo di questa sezione è fornire le Istruzioni Operative per la gestione dei Personal Computer.

Non è consentito che due o più Incaricati al trattamento accedano al sistema, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente e la medesima password.

Il periodo massimo di non utilizzo della password da parte dell'Incaricato è stabilito in tre mesi.

Al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza l'incaricato non deve lasciare incustodito e accessibile lo strumento elettronico. Quindi nel caso in cui ci si allontani dalla postazione si dovrà attivare lo screensaver o idonei mezzi di protezione messi a disposizione dalla Fondazione che impediscano l'accesso ai dati presenti nel PC. Quando vi è necessità di assentarsi in modo prolungato dalla propria postazione di lavoro, oltre che attivare gli idonei mezzi di protezione sopra citati, si consiglia, ove possibile, di chiudere a chiave la porta quando si esce dalla stanza.

L'ASL Roma B non risponderà della perdita dei dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro, il cui trattamento in ogni caso non deve interferire con la normale attività lavorativa. In particolare tali dati non potranno essere salvati nei server aziendali.

Ulteriori disposizioni e/o informazioni sono contenute nella procedura informatica pubblicata nell'area intranet aziendale.

ISTRUZIONI PER LA GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI

Lo scopo di questa sezione è di fornire le Istruzioni Operative riguardanti la gestione dei supporti di memorizzazione rimovibili: hard disk dei personal Computer, CD ROM, floppy disk .

Prima di procedere al riutilizzo per altri scopi dei supporti di memorizzazione e nel caso fosse necessario conservare le informazioni contenute negli stessi, deve essere effettuato il salvataggio dei dati.

I supporti di memorizzazione prima di essere riutilizzati, devono essere completamente reinizializzati, di modo che le informazioni precedentemente contenute non siano recuperabili e tecnicamente ricostruibili in alcun modo.

Gli Incaricati al trattamento dei dati personali hanno la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 10 di 13
PROCEDURE PRIVACY PER INCARICATI				

- segnalare la necessità di un'eventuale dismissione dei floppy disk;
- segnalare la necessità di un'eventuale riutilizzo degli hard disk, dei CD-ROM e dei floppy disk;
- eseguire la reinizializzazione dei floppy disk per poterli successivamente riutilizzare;
- effettuare il test sulla reinizializzazione dei floppy disk eseguita precedentemente.

ISTRUZIONI PER IL TRATTAMENTO DEI DOCUMENTI CARTACEI

Lo scopo di questa sezione è evidenziare le norme che gli Incaricati al trattamento dei dati personali devono applicare e rispettare quando trattano documenti cartacei contenenti Dati Personali e/o Sensibili e/o Giudiziari.

Gli Incaricati hanno l'obbligo, durante lo svolgimento dell'attività di trattamento dei documenti, di applicare le norme riportate di seguito e le direttive emanate dal Responsabile del trattamento.

Gli Incaricati devono operare in modo da consentire l'accesso esclusivamente:

- all'Interessato a cui tali dati si riferiscono;
- al Responsabile del trattamento di quella tipologia di dato;
- agli altri Incaricati a trattare quella tipologia di dato.

Nel caso specifico è richiesto di:

- trattare i Dati Personali e/o Personali Sensibili secondo il principio di necessità, ovvero unicamente per lo scopo per cui sono stati raccolti;
- non diffondere o comunicare i Dati Personali e/o Personali Sensibili a soggetti non autorizzati al trattamento;
- non lasciare incustoditi documenti contenenti Dati Personali e/o Personali Sensibili durante e dopo l'orario di lavoro;
- non lasciare in luoghi accessibili al pubblico i documenti contenenti Dati Personali e/o Personali Sensibili;
- riporre i documenti negli archivi quando non più operativamente necessari;
- limitare allo stretto necessario l'effettuazione di copie dei suddetti documenti.

La riproduzione di documenti contenenti Dati Personali Sensibili su supporti non informatici (ad esempio fotocopie) è vietata se non espressamente autorizzata preventivamente e

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 11 di 13
PROCEDURE PRIVACY PER INCARICATI				

specificatamente dalla Direzione Sanitaria, Responsabile competente o se richiesta dal paziente. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali.

Nel seguito sono evidenziate le disposizioni che il Responsabile del trattamento e gli Incaricati al trattamento devono applicare e rispettare quando trattano documenti cartacei contenenti Dati Personali e/o Personali Sensibili.

ARCHIVAZIONE DEI DOCUMENTI CARTACEI

I documenti cartacei devono essere:

- tenuti in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti, garantendo, quindi, la riservatezza e l'integrità dei Dati Personali e/o Personali Sensibili, in essi contenuti;
- riposti negli appositi archivi che dovranno essere chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa;
- le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;
- trasferiti presso gli archivi centrali quando non più operativamente necessari.

In particolare, a titolo esemplificativo, si evidenziano nella tabella sottostante alcune disposizioni da osservare:

<i>Tipo documento</i>	<i>Disposizione</i>
Cartelle Cliniche	Il documento deve, quanto più possibile, viaggiare insieme al paziente cui si riferisce
Cartelle Cliniche	Il documento deve essere utilizzato in maniera che i dati relativi al paziente siano visibili solo a chi è autorizzato a trattarli (Es. deve essere appoggiato sempre con il frontespizio rivolto verso il basso, ecc.)

CONSULTAZIONE DEI DOCUMENTI CARTACEI

La consultazione dei documenti, contenenti Dati Personali e/o Personali Sensibili, deve avvenire esclusivamente da parte degli Incaricati al trattamento, solo quando operativamente necessario e, quando possibile, in loco.

L'Incaricato al trattamento può effettuare la consultazione di tali documenti fuori orario di lavoro, solo se preventivamente autorizzato dal Responsabile, identificato e registrato dalla vigilanza.

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 12 di 13
PROCEDURE PRIVACY PER INCARICATI				

CONSEGNA DEI DATI AGLI INTERESSATI

La consegna dei documenti contenenti Dati Personali e/o Personali Sensibili deve essere effettuata, in modo da garantirne la riservatezza, in busta chiusa indirizzata nominativamente al destinatario (Responsabile, Incaricato e/o Interessato).

DISTRUZIONE DEI DOCUMENTI CARTACEI

Tutti i documenti che non devono essere conservati per legge devono essere distrutti al termine della loro utilizzazione.

La distruzione dei documenti cartacei, nei limiti consentiti dalla legge, deve essere effettuata quando è espressamente richiesto dall'Interessato e/o quando comunicato dal Responsabile del trattamento, all'interno della propria area di competenza.

I documenti dovranno essere distrutti, sotto la supervisione del Responsabile del Trattamento, all'interno della propria unità.

La distruzione dei documenti cartacei contenenti Dati Personali Sensibili deve essere effettuata, attraverso opportuni strumenti, in modo da rendere impossibile la ricostruzione del documento.

Revisione n. 0	Documento ASL Roma B UOC Qualità	Cod. Doc. Py 2 - 06		Pagina 13 di 13
PROCEDURE PRIVACY PER INCARICATI				

Allegato 1 RACCOMANDAZIONI PER LA CREAZIONE DELLE PASSWORD

Raccomandazioni per la creazione delle Password

1. Le password dovrebbero essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.
2. Le password dovrebbero contenere almeno un carattere appartenente a ciascuno degli insiemi sopra enunciati.
3. Nei casi in cui non risulti possibile l'utilizzo dei simboli speciali, le password dovrebbero contenere caratteri numerici ed alfabetici ripartibili in numero compreso tra un minimo di 3 ed un massimo di 5, ferma restando la lunghezza minima complessiva fissata in 8 caratteri.
4. Le password non dovrebbero contenere più di 3 caratteri uguali consecutivi.
5. Le password non dovrebbero contenere caratteri di spaziatura.
6. Le password non dovrebbero contenere:
 - a. nomi propri di persona;
 - b. sigle di funzioni organizzative o progetti interni alla Fondazione;
 - c. nomi di giorni della settimana, mesi dell'anno o stagioni;
 - d. nomi di riferimenti geografici;
 - e. nomi di personaggi della politica, sport, cinema e fumetti.
 - f. riferimenti al corrispettivo identificativo utente;
 - g. il nome o cognome dell'incaricato;
 - h. la matricola dell'incaricato;
 - i. la data di nascita dell'incaricato;
 - j. esclusivamente date in qualsiasi formato e con qualsiasi separatore di uso comune.
7. Ogni nuova password dovrebbero differire dalla precedente perlomeno in 4 caratteri.