NORME AD USO DEGLI INCARICATI PER IL TRATTAMENTO DEI DATI CON STRUMENTI ELETTRONICI

EDIZIONE 2012

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

INDICE

1 INTRODUZIONE.....3

2 VADEMECUM PER GLI INCARICATI DEI TRATTAMENTI DEI DATI EFFETTUATI CON STRUMENTI ELETTRONICI.....4

2.1 Norme ad uso dei singoli operatori delle postazioni di lavoro basate su computer 4

2.1.1 Comportamenti a rischio 5

2.2 Uso del supporto rimovibile (di tipo floppy disk, cd-rom, pen drive, etc.).....6

3 REGOLE DI CONDOTTA PER I RESPONSABILI E GLI INCARICATI E LICEITA' DEI RELATIVI TRATTAMENTI.....8

3.1 Impegni dei Responsabili, Incaricati ed Addetti.....8

3.2 Doveri dei Responsabili, Addetti ed Incaricati.....9

3.3 Tenuta ed aggiornamento dei dati.....9

3.4 Acquisizioni da fonti orali.....9

3.5 Raccolta dei dati.....10

3.6 Classificazione dei dati.....10

3.7 Credenziali.....10

4 NORME PER LA SICUREZZA DELLE INFORMAZIONI.....12

4.1 Norme per la miglior sicurezza nel trattamento dei dati.....12

4.2 Norme per la prevenzione dei virus informatici.....14

4.3 Norme che riguardano la parola chiave.....15

4.4 Alcune norme generiche di sicurezza e protezione dati personali.....17

4.5 Norme che riguardano i sistemi informatici aziendali.....18

4.5.1 Utilizzo del personal computer.....18

4.5.2 Utilizzo di supporti magnetici.....18

4.5.3 Utilizzo della rete aziendale.....19

4.5.4 Utilizzo della rete Internet e dei relativi servizi.....19

4.5.5 Utilizzo della Posta Elettronica.....19

4.5.6 Registrazione accessi.....21

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

1 INTRODUZIONE

Lo scopo del documento è di fornire un insieme di istruzioni operative agli incaricati del trattamento dei dati che fanno uso di strumenti elettronici al fine di ottemperare a quanto previsto nell'articolo 34 del Decreto Legislativo 196/03 in tema di Misure Minime di Sicurezza da adottare per la protezione dei dati.

Il documento, inoltre, costituisce l'insieme delle istruzioni impartite dal Titolare agli incaricati dei trattamenti ai sensi degli articoli 29 e 30 del Decreto Legislativo 196/03.

Infine, il documento costituisce lo strumento didattico volto alla formazione degli incaricati dei trattamenti.

In allegato al presente documento vengono riportati alcuni articoli del Decreto Legislativo 196/03 e del relativo disciplinare tecnico (allegato B).

In particolare nel capitolo 2 viene riportato un Vademecum strutturato in punti in cui sono indicate le diverse norme da seguire a cura degli Incaricati che utilizzano strumenti elettronici per i trattamenti dei dati. Si tratta, in tal caso, sia di norme generali di sicurezza della postazione di lavoro che di norme riguardanti l'accesso ad Internet e l'utilizzo delle e-mail nonché le procedure da seguire per l'effettuazione delle copie di backup.

Nel capitolo 3 sono riportate delle regole di condotta da parte dei Responsabili e degli Incaricati del trattamento dati.

Nel capitolo 4 sono riportate le Nome relative alla sicurezza dei dati che in parte ricalcano quanto già descritto nei capitoli precedenti ma fornendone una visione unitaria.

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

2 VADEMECUM PER GLI INCARICATI DEI TRATTAMENTI DEI DATI EFFETTUATI CON STRUMENTI ELETTRONICI

2.1 NORME AD USO DEI SINGOLI OPERATORI DELLE POSTAZIONI DI LAVORO BASATE SU COMPUTER

1. La sicurezza totale non esiste: informatevi, tenetevi aggiornati, prevenite, evitate le cattive abitudini di lavoro;

2. Considerate il PC come un oggetto personale sia in Azienda che in casa, alla stregua di carte di credito, carta d'identità, ecc. Non consentitene l'utilizzo a chiunque e, nel caso di problemi hardware o software che comportino la necessità d'interventi esterni, rivolgetevi sempre alle persone autorizzate dalla UOC Sistema Informativo e Sistema di Reporting Aziendale ed ICT (d'ora in avanti nel documento ICT);

3. Attuate sempre una valida protezione hardware di base, ponendo una o più etichette adesive autografate sulle viti posteriori del cabinet (la stessa tecnica viene attuata dal personale ICT preposto alla manutenzione e consegna dell'hardware per controllare l'invalidazione delle garanzie);

4. Le postazioni informatiche condivise da più utenti e configurate come terminale ovvero postazioni che non hanno diritto ad accedere ad aree dati se non attraverso autenticazione, non devono essere utilizzate per l'archiviazione locale di dati personali o sensibili alla privacy;

5. Modificate periodicamente le password ed evitate di affidare a Windows la memorizzazione automatica delle stesse (posta elettronica, accesso remoto, etc.). Tutte le password gestite direttamente dal sistema operativo Windows sono altamente insicure. E' consigliabile digitare la password ogni volta che questi servizi vengono utilizzati;

6. Evitate, possibilmente, di usare la connessione ad Internet con un PC contenente dati riservati e/o personali. Se è inevitabile la connessione, mantenete attivo in background l'antivirus aziendale che è costantemente aggiornato. Impostate o pretendete impostati i livelli di sensibilità e di protezione al massimo. L'eventuale attivazione di un firewall personale deve essere assolutamente autorizzata dall'ICT in quanto la cattiva configurazione dello stesso potrebbe compromettere il funzionamento dei servizi IT aziendali al punto da creare, per assurdo, problemi di sicurezza impedendo, per esempio, all'antivirus centralizzato di attivarsi o aggiornarsi;

7. Mentre navigate prima di selezionare un link, posizionateci sopra il cursore del mouse e osservatene il percorso sulla apposita barra del browser: se è un file eseguibile probabilmente è un trucco per farvi scaricare un dialer o peggio. In particolar modo fate attenzione a tutte i messaggi provenienti dal browser che richiedono l'apertura, l'installazione o il salvataggio di files;

8. Eseguite periodicamente la pulizia del disco da cookies, file temporanei, etc.;

9. Fate attenzione ai messaggi di posta elettronica in formato "html" verificandone la provenienza in quanto, seppure consentano una forma più elegante e/o simpatica, è uno dei metodi più subdoli per veicolare contenuti di virus, worm e frodi (senza necessità di allegati);

10. Non rispondete ai messaggi di posta elettronica provenienti da indirizzi a voi non noti, chiedendo per esempio di essere cancellati da quella lista di invio: in tal modo rischiate di

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163
REGIONE LAZIO

fare il gioco di chi li ha spediti, facendogli capire che la vostra casella di posta è attiva. Aggiungete, anzi, tali indirizzi tra quelli indesiderati;

11. Non comunicate la vostra e-mail a siti ai quali non siete veramente interessati e/o sui quali avete anche il minimo dubbio;
12. Evitate i falsi allarmi e di rispondere alle cosiddette "catene di S. Antonio" in quanto tali tecniche vengono utilizzate per saturare la rete dati e rendere di conseguenza inefficiente i servizi Internet e di Posta Elettronica.

2.1.1 Comportamenti a rischio

Sono comportamenti a rischio:

1. la navigazione su siti di Hacking, Cracking, ecc...;
2. scaricare software da siti poco attendibili o non ufficiali;
3. aprire messaggi di posta elettronica ed eseguire files allegati ai messaggi senza preventiva scansione antivirus (anzi, prima si dovrebbe effettuare l'aggiornamento e poi si dovrebbe aprire il programma di posta elettronica);
4. installare programmi scaricati da siti non ufficiali o comunque di natura incerta;
5. dar credito a un messaggio pubblicitario dalle caratteristiche sospette (spesso di natura erotica o che promette facili guadagni) che reindirizza ad un sito internet "per saperne di più";

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

2.2 Uso del supporto rimovibile (di tipo floppy disk, cd-rom, pen drive, etc.)

Tutti gli *Incaricati* che trattano dati *sensibili:*

In linea generale, non viene raccomandata la copia su supporti rimovibili di dati sensibili e giudiziari per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.

Non si deve inoltre dimenticare che tale supporto di archiviazione, smarrito e/o accidentalmente lasciato incustodito, anche per breve periodo, può essere rapidamente letto e copiato, senza lasciare alcuna traccia dell'accaduto. Ci troviamo quindi davanti ad un rischio concreto di accesso non autorizzato o copia abusiva dei dati sensibili.

Ciò premesso, ove nello svolgimento della normale attività assegnata all'*Incaricato*, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di dati *sensibili*, occorre attenersi alle seguenti cautele:

1. Accertarsi che i supporti siano debitamente formattati e privi di altri file. Nel dubbio, è sempre bene provvedere alla formattazione ex novo prima di registrare dati sensibili;

2. Per evitare l'alterazione dei dati in questione, dopo la copia, si attivi la protezione contro possibili nuove scritture, che potrebbero alterare i dati stessi;

3. Il supporto deve essere contrassegnato da un'etichetta, riportante un'indicazione in chiaro od in codice, tale da permettere all'*Incaricato* di riconoscerne immediatamente il contenuto, ed evitare che egli possa confonderlo con altri simili che probabilmente sono in suo possesso per via della normale attività lavorativa;

4. Il supporto di archiviazione non deve mai essere lasciato incustodito, ma è sempre direttamente e personalmente conservato dall'Incaricato che ha realizzato la copia. Esso deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato; in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte idonea alla custodia di supporti ottici e/o magnetici.

5. In caso di spedizione ad altro *Incaricato*, occorre accertarsi che il destinatario abbia lo stesso profilo d'autorizzazione del mittente e che il supporto venga spedito in una busta sigillata, intestata personalmente all'*incaricato*, con controfirma sul lembo di chiusura; ove i dati siano particolarmente sensibili, si deve utilizzare una apposita busta, dotata di sigillo in plastica induplicabile e con numerazione univoca, per metter in evidenza qualsiasi tentativo di violazione;

6. Non si devono trasmettere supporti di archiviazione, contenenti *dati sensibili* ad un destinatario, senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura, che permette di confermare l'avvenuta consegna al destinatario del supporto;

7. Quando sono registrati dati relativi all'identità genetica di una persona, la creazione del supporto è eseguita all'interno d'un locale protetto da occhi indiscreti ed occorre a priori una disposizione in deroga, scritta del *Responsabile* o dal *Titolare*; inoltre la registrazione dei dati sui supporti deve avvenire in forma cifrata, indipendentemente dal rispetto delle istruzioni di spedizione sopra illustrate;

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

8. Qualora i dati contenuti non abbiano più ragione di essere, si deve provvedere immediatamente alla sua cancellazione o alla formattazione dei supporti ed all'asportazione dell'etichetta con l'indicazione del contenuto;

9. Poiché i supporti, generalmente sono particolarmente sensibili ai campi magnetici, allo scopo d'evitare la cancellazione o danneggiamento anche accidentale dei dati, gli stessi non devono mai essere avvicinati ad un campo magnetico, come ad esempio il magnete d'un altoparlante, oppure lasciati abbandonati nelle vicinanze di un trasformatore elettrico, come quelli utilizzati nelle lampade da tavolo, in quanto i campi dispersi potrebbero danneggiare il contenuto dei supporti;

10. I supporti non devono mai essere esposti ad estremi di temperatura e d'umidità; in particolare non devono essere lasciati esposti al sole in un'autovettura chiusa e, qualora debba essere trasportato da un ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura significativo, prima dell'utilizzo è necessario lasciare passare un adeguato intervallo di tempo, allo scopo di permettere all'eventuale condensa di dissolversi;

11. Si faccia sempre attenzione a non dimenticare i supporti anche all'interno del computer, quando, al termine della copia, si spegne la macchina o ci si allontana per qualsiasi motivo;

12. Qualora il contenuto dei supporti debba essere copiato su un hard disk, o altro strumento elettronico di trattamento, ci si accerti di cancellare il relativo contenuto al termine dell'operazione di trattamento; si presti una particolare attenzione a che nessun dato sia rimasto nella memoria buffer, nella clipboard, negli appunti o all'interno del cestino, specie in sistemi operativi di tipo Microsoft Windows;

13. Se l'operazione è ragionevolmente possibile, si raccomanda vivamente di compilare un registro con l'indicazione numerica, o con altro contrassegno, ove sono riportati tutti i supporti contenenti dati sensibili, la loro ubicazione, le modalità d'accesso e gli eventuali estremi di consegna ad altro incaricato autorizzato;

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

3 REGOLE DI CONDOTTA PER I RESPONSABILI E GLI INCARICATI E LICEITA' DEI RELATIVI TRATTAMENTI

1. Nel trattare i dati di carattere personale, *Responsabili*, *Addetti* ed *Incaricati* adottano, in armonia con la legge ed i regolamenti, le modalità più opportune idonee a favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati.

2. *Responsabili*, *Addetti* e *Incaricati,* si adoperano per il pieno rispetto, anche da parte dei terzi con cui entrano in contatto, delle disposizioni che tutelano il *segreto d'azienda* – è fatto assoluto divieto divulgare anche verbalmente notizie o file che riguardano il lavoro svolto.

3. *Responsabili*, *Addetti* e *Incaricati,* che gestiscono anche archivii elettronici, nel trattare i file contenenti *dati sensibili*, s'attengono ai doveri di lealtà, liceità, correttezza, imparzialità, onestà e diligenza propri dell'esercizio della funzione o della qualifica o livello ricoperti. Essi conformano il proprio comportamento al principio di trasparenza dell'Attività Aziendale.

4. *Responsabili*, *Addetti* e *Incaricati,* che operano a contatto col pubblico e ricevono a vario titolo i file contenenti *dati personali* relativi alle casistiche sopra riportate, devono sempre compilare e far compilare la prescritta modulistica informativa accompagnatoria. Avranno inoltre sempre cura di archiviare la documentazione completa in ogni sua parte.

3.1 Impegni dei Responsabili, Incaricati ed Addetti

Responsabili, Incaricati ed Addetti si impegnano a:

1. Favorire il recupero, l'acquisizione e la tutela dei file contenenti dati personali. A tal fine, operano in conformità con i principi, i criteri metodologici e le pratiche, generalmente condivisi ed accettati, curando anche l'aggiornamento sistematico e continuo delle proprie conoscenze storico/amministrative;

2. Tutelano l'integrità degli archivi elettronici e l'autenticità dei file di cui sono addetti alla tenuta, nei termini stabiliti, in particolare di quelli esposti a rischi di distruzione, cancellazione, dispersione ed alterazione dei dati;

3. Salvaguardare la conformità delle riproduzioni dei file agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati (attuare le protezioni del tipo "file protetto da revisioni con password", "file di sola lettura", ecc..)

4. assicurare il rispetto delle misure minime di sicurezza previste dall'allegato B del Codice della Privacy e successive integrazioni e modificazioni, sviluppando misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai file e adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni file e la conservazione degli originali in partizioni protette secondo le disposizioni ricevute dal Responsabile del trattamento.

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

3.2 Doveri dei Responsabili, Addetti ed Incaricati

Responsabili, Addetti ed Incaricati devono:

1. non fare alcun uso dei file contenenti informazioni ottenute in ragione della propria attività, anche in via confidenziale, per proprie ricerche, propri fini o per realizzare profitti e interessi privati. Nel caso in cui *Responsabili*, *Addetti* e *Incaricati* svolgano ricerche o sondaggi d'opinione per scopi commerciali o altro, che è indicato dal *Titolare* del trattamento, ciò è soggetto alle stesse regole ed ai medesimi limiti previsti dalla documentazione che ha dato origine per finalità all'acquisizione dei dati stessi;

2. mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attività;

3. *Responsabili*, *Addetti* e *Incaricati,* osservano tali **doveri di riserbo** anche dopo la cessazione dalla propria attività, sia per trasferimento ad altro incarico sia per fine del Rapporto di Lavoro;

3.3 Tenuta ed aggiornamento dei dati

1. *Responsabili*, *Addetti* e *Incaricati,* favoriscono l'esercizio del diritto degli *interessati* all'aggiornamento, alla rettifica od all'integrazione dei dati (artt. 7 – 8 del D.Lgs n. 196 datato 30.6.2003), garantendone la conservazione secondo modalità che assicurano la distinzione delle fonti originarie dalla documentazione successivamente acquisita;

2. Ai fini dell'applicazione dell'art. 7 del D.Lgs n. 196 datato 30.6.2003, in presenza d'eventuali richieste generalizzate d'accesso ad un'ampia serie di dati o documenti, *Responsabili*, *Addetti* ed *Incaricati* sfruttano tutti gli strumenti di ricerca e le fonti pertinenti, fornendo al richiedente idonee indicazioni per una loro agevole consultazione.

3. In caso d'esercizio di un diritto, ai sensi dell'art. 8 del Codice, da parte di chi vi ha *interesse* a proposito di *dati personali* che riguardano dipendenti, persone decedute e file contenenti informazioni/documenti assai risalenti nel tempo, la sussistenza dell'interesse è valutata anche per riferimento al tempo trascorso;

4. l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati" riguardano espressamente anche i trattamenti effettuati senza l'ausilio di strumenti elettronici;

5. Oggetto di trattamento sono i dati personali, cioè qualsiasi informazione su un soggetto.

3.4 Acquisizioni da fonti orali

1. In caso di trattamento per acquisizione da *fonti orali*, è necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente anche in forma verbale sulla base di *un'informativa semplificata* (modello indicato dall'Azienda), che l'operatore compila e renda nota almeno l'identità e l'attività svolta dall'intervistatore nonché le finalità della raccolta dei dati.

2. *Responsabili*, *Addetti* e *Incaricati,* che acquisiscono da *fonti orali,* richiedono all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo *consenso* manifestato dagli intervistati.

3.5 Raccolta dei dati

Responsabili, *Addetti* e *Incaricati* della *raccolta dati* si attengono alle disposizioni contenute nel presente dispositivo, del D.Lgs n. 196 datato 30.6.2003*,* ed alle istruzioni verbali impartite quotidianamente, ed in particolare:

1. *Responsabili*, *Addetti* e *Incaricati* rendono nota all'*interessato* la propria identità, la funzione e le finalità della raccolta, attraverso l'adeguata documentazione (consenso, informativa ecc.);

2. *Responsabili*, *Addetti* e *Incaricati* forniscono all'*interessato* le informazioni di cui agli artt. 7 – 8 - 13 del D.Lgs n. 196 datato 30.6.2003 e ogni altro chiarimento che consenta allo stesso di rispondere in modo adeguato e consapevole, dovranno evitare comportamenti che possano configurarsi come artificiosi od indebite pressioni;

3. *Responsabili*, *Addetti* e *Incaricati* non possono svolgere contestualmente presso gli stessi *interessati* attività di rilevazione di dati per conto di più *titolari,* salvo espressa autorizzazione del *Titolare,* citando nell'informativa e nel consenso la causale;

4. *Responsabili*, *Addetti* e *Incaricati* provvedono tempestivamente alla correzione degli errori e delle inesattezze contenute nei file circa le informazioni acquisite nel corso della raccolta;

5. *Responsabili*, *Addetti* e *Incaricati* assicurano una particolare osservanza dei regolamenti e pongono maggiore diligenza nella raccolta specifica per la memorizzazione su file informatici, di *dati personali* ed eventualmente classificati *sensibili o giudiziari*.

3.6 Classificazione dei dati

La classificazione deve essere fatta in modo tale da poter essere applicata ad un bene (i dati) indipendentemente dal media ove questo sia contenuto. In tal senso deve essere prevista anche una attività di etichettatura dei supporti di memorizzazione:

Classificazione informazioni :

a) Non Classificate

b) Confidenziali

c) Riservate

d) Ad uso interno

e) Dati Personali

f) Dati Sensibili o Giudiziari.

3.7 Credenziali

Una credenziale si compone di:

1. Nome utente, ovvero, con il termine inglese, username,

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

2. Parola chiave, ovvero, con il termine inglese, password.

Si tratta della modalità attraverso la quale l'Azienda consente ai propri Incaricati di utilizzare determinati servizi informatici/applicativi (trattamenti) presenti all'interno dei propri sistemi informativi. Nel caso di un sistema che tratti i dati personali e sensibili la username e la password devono essere sottoposte a policy ancor più forti e definite nel paragrafo relativo nel presente documento e/o emanate dalla struttura ICT.

Gli incaricati dei trattamenti a cui vengono fornite dall'Azienda credenziali che gli consentano l'accesso a determinati sistemi operativi o a determinati applicativi dovranno attenersi strettamente alle norme generali descritte nel presente documento.

Inoltre, dovranno attenersi strettamente alle seguenti disposizioni:

1. Il nome utente e la parola chiave sono assolutamente personali, non devono essere comunicati ad alcuno, neppure nel caso di colleghi che hanno le medesime autorizzazioni; nel caso di assenze prolungate valgono le disposizioni contenute nel paragrafo "Norme che riguardano la parola chiave" del presente documento e/o emanate dalla struttura ICT.
2. L'utente è tenuto a conservare le credenziali in maniera scrupolosa attenendosi alle norme di cui al paragrafo "Norme per la miglior sicurezza nel trattamento dei dati" in maniera tale da evitare la sottrazione delle stesse ad opera di un altro operatore o di un soggetto esterno all'ospedale con strumenti informatici e non.

Qualora fosse appurato il verificarsi di sottrazioni di credenziali ad un operatore a causa di carenza di consapevolezza, disattenzione o incuria ed altri comportamenti dello stesso non conformi a quanto definito dalle norme di cui sopra, verranno presi provvedimenti adeguati e nei casi più gravi il ricorso all'autorità giudiziaria.

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

4 NORME PER LA SICUREZZA DELLE INFORMAZIONI

Questo capitolo ha lo scopo di fornire agli ***incaricati*** **ed** ***addetti*** **del trattamento** una panoramica sulle responsabilità loro spettanti, e far conoscere la policy relativa alla gestione e sviluppo della sicurezza dell'informazione.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

1. **Riservatezza**: prevenzione contro l'accesso non autorizzato alle informazioni;
2. **Integrità**: le informazioni non devono essere alterabili da incidenti o abusi;
3. **Disponibilità**: il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche di opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate sul disco fisso di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

4.1 Norme per la miglior sicurezza nel trattamento dei dati

1. Utilizzate le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete (da considerare che potrebbe essere lecito l'accesso nella stanza da parte di personale non autorizzato alla consultazione dei dati sensibili, es. personale pulizie, tecnici assistenza, etc.).

2. Conservate i supporti rimovibili in un luogo sicuro

Per i supporti rimovibili si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, vanno riposti sotto chiave non appena avete finito di usarli.

3. Utilizzate le password

Esistono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) La password di accesso al dominio di rete aziendale impedisce che l'eventuale utilizzo non autorizzato di una postazione renda disponibili tutte le risorse di rete, a tal proposito è necessario disconnettere la propria utenza in caso di non utilizzo della postazione informatica onde salvaguardare la riservatezza dei propri dati e di quelli aziendali.

b) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato;

Nota: Imparate ad utilizzare questi tipi fondamentali di password, e mantenete distinta almeno quella di tipo "a", che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Successivamente all'assistenza cambiate la password.

4. Attenzione alle stampe di documenti contenenti dati sensibli

Non lasciate accedere ai supporti o ai file le persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe ottenute. Distruggete personalmente le stampe, formattate i supporti e distruggete i file quando non servono più.

5. Non lasciate traccia dei file con dati riservati

Generalmente nei sistemi operativi come Windows quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Verificate sempre l'avvenuta cancellazione dei file controllando la sua assenza nel "cestino".

6. Prestate attenzione all'utilizzo dei PC portatili

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un PC portatile, fatevi installare un buon programma di cifratura del disco rigido (hard-disk) e utilizzate una procedura di backup periodico.

7. Non fatevi spiare quando state digitando le password

Anche se i programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

8. Custodite le password in un luogo sicuro

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

9. Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identitá

Personale esterno o della manutenzione interna può avere bisogno di installare del nuovo software/hardware nel vostro computer.

Assicuratevi dell'identità della persona (se non conosciuta) e delle autorizzazioni ad operare sul vostro PC.

10. Non utilizzate apparecchi non autorizzati

L'eventuale utilizzo di modem o chiavette internet su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi vietato. Per l'utilizzo di altri apparecchi, consultatevi con il Responsabile del trattamento dati del vostro ufficio.

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

11. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi Aziendali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il Responsabile del trattamento dati.

12. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni macchina contratte da virus informatici sul vostro computer ancor che obbligatoria, è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus informatico; tra l'altro, potreste incorrere in una perdita irreparabile di dati e gravi danni al sistema ed alla rete.

13. CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP

I vostri dati potrebbero essere gestiti da un *file server* oppure in disco locale e trasferiti in un server solo al momento del backup. Consultate la struttura ICT per farvi aiutare nella migliore soluzione architetturale che tuteli i vostri dati.

14. EFFETTUATE L'AGGIORNAMENTO DEI SISTEMI ANTIVIRUS

Controllate che l'antivirus istallato sia il più aggiornato possibile. Verificate periodicamente che gli aggiornamenti avvengano non oltre le due settimane, in modo da preservare il vostro PC da virus di ultima generazione. Nel caso di eventuali allarmi virus, attenetevi scrupolosamente alle istruzioni che vi saranno comunicate dal servizio tecnico attraverso le linee guida.

4.2 NORME PER LA PREVENZIONE DEI VIRUS INFORMATICI

Un virus informatico è un programma in grado di trasmettersi o replicarsi autonomamente e che può causare effetti dannosi. Alcuni virus informatici si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido e possono causare gravi danni alla rete.

- **COME SI TRASMETTE UN VIRUS:**
  - Attraverso programmi provenienti da fonti non ufficiali o dalle macro dei programmi di automazione d'ufficio (es. Word, Excel, ecc);
  - attraverso la rete;
  - attraverso la navigazione sul Web;
  - attraverso dispositivi asportabili.
- **QUANDO IL RISCHIO DA VIRUS SI FA SERIO:**
  - Quando si installano programmi, specie se non autorizzati o sicuri;
  - Quando si copiano dati da floppy-disk, dvd-rom, cd-rom e chiavette USB non sicuri o di provenienza sconosciuta;
  - Quando si scaricano dati o programmi da Internet.
- **QUALI EFFETTI HA UN VIRUS?**
  - I possibili effetti dei virus sono quanto mai disparati. Dei possibili esempi sono:

- effetti sonori e messaggi sconosciuti appaiono sul video;
- attivazione/disattivazione automatica di applicazioni;
- problemi nell'accensione del computer;
- cancellazione di file dall'hard disk;
- il computer diventa inutilizzabile presentando un grave errore di sistema;
- il computer rallenta pesantemente le prestazioni (diventa "lenta").

- **COME PREVENIRE I VIRUS:**
  - **USARE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**

    Copie sospette di programmi possono contenere virus informatici o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima d'essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus informatici.
  - **ASSICURATEVI DI NON FAR PARTIRE IL VOSTRO COMPUTER DA SUPPORTI RIMOVIBILI**

    Infatti se il supporto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
  - **PROTEGGETE I VOSTRI SUPPORTI RIMOVIBILI DA SCRITTURA QUANDO POSSIBILE**

    In questo modo eviterete le scritture accidentali, magari tentate da un virus informatico che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.
  - **NON DIFFONDETE MESSAGGI VIA E-MAIL DI PROVENIENZA DUBBIA**

    Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo e non inoltratelo assolutamente: le e-mail di questo tipo sono dette con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico.

    È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM, le poste, la banca... (sono gli *hoax* più diffusi).
  - **NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI**

    Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

4.3 NORME CHE RIGUARDANO LA PAROLA CHIAVE

- **SCELTA DELLE PASSWORD**

  Il più semplice metodo per l'accesso illecito ad un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema

informativo ed alle reti a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

- **COSA FARE**
  - **NON** dite a nessuno la vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le vostre risorse o possa farlo a vostro nome.
  - **NON** scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
  - Quando immettete la password **NON** fate sbirciare a nessuno quello che state battendo sulla tastiera.
  - **NON** scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
  - **NON** crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
  - **NON** usate il vostro nome utente. È la password più semplice da indovinare.
  - **NON** usate password che possano in qualche modo essere legate a voi come, ad esempio, il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc..
  - Cambiate la password al primo accesso e successivamente ad intervalli regolari. **In caso in cui l'applicazione dovesse consentire l'accesso a dati sensibili la password dovrà essere modificata almeno ogni tre mesi. Negli altri casi almeno ogni sei mesi.**
  - Usate password lunghe almeno otto caratteri o il massimo consentito dal sistema con un misto di lettere, numeri e segni di interpunzione laddove il sistema lo consenta.
  - Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri".
  - Il tipo di password in assoluto più sicura è quella associata ad un supporto d'identificazione come un cd-rom, floppy-disk, un mini hard-disk USB, una carta a microprocessore.
  - In caso di dubbio, consultate l'amministratore di sistema della struttura ICT.

- **COME SCEGLIERE UNA PASSWORD**

  Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase "C'era una volta una gatta che aveva una macchia nera sul muso" può ad esempio fornire, tra le tante possibilità, "Cr1Vlt1Gtt". Ecco alcuni altri esempi:

Frase	Possibile password
57% di Finlandesi hanno detto si alla EU	57%DFNHDSAEU
Roma è la capitale d'Italia	RMCPIEST
La mia macchina costa 27 milioni	MOPL27KKL
Meglio un uovo oggi che una gallina domani	MGLO/GLND
To be or not to be	(2B)V(!2B)
Nel 1970 ho traslocato a Roma	I70I->RM
"Esc" si trova in alto a sinistra	"E"stULK
Gnu è un acronimo ricorsivo	GstACRR
Tutto è bene quel che finisce bene	2TBCFNB

- **IN CASO DI ASSENZA PROLUNGATA**

  Nel caso in cui un incaricato dovesse essere assente improvvisamente o in maniera programmata, la persona incaricata come sostituto verrà dotata, di nuove credenziali conosciute soltanto dal sostituto le quali saranno appartenenti al medesimo profilo autorizzativo di quelle dell'assente, che metteranno il sostituto nelle condizioni di agire in vece dell'assente ma senza la conoscenza della parola chiave. Per alcun motivo si potranno comunicare le proprie credenziali di accesso ad altri operatori.

4.4 ALCUNE NORME GENERICHE DI SICUREZZA E PROTEZIONE DATI PERSONALI

Al lavoro presso la vostra postazione, orientate lo schermo del video in modo da non essere "letto" a distanza a vostra insaputa. Al termine della giornata lavorativa ed in caso d'assenza temporanea dal posto di lavoro (pausa pranzo, riunioni, ecc.) è necessario:

1. Riporre tutta la documentazione ed i supporti fisici contenenti dati personali negli armadi, nelle cassettiere personali o negli archivi all'uopo predisposti;

2. Spegnere i terminali e disconnettere la propria sessione sui PC;

3. Impedire l'accesso a tutti i PC e terminali attraverso l'impiego generalizzato di password e, ove previsto, dell'apposita serratura di disattivazione;

4. Custodire presso di sé o in luogo sicuro le chiavi delle serratura di disattivazione;

5. Custodire le chiavi delle serrature dei mobili, uffici e computer in posizioni non evidenti o facilmente identificabili da estranei.

4.5 Norme che riguardano i sistemi informatici aziendali

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne di comportamento comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto:

1. tali strumenti vanno custoditi in modo appropriato;
2. tali strumenti possono essere utilizzati solo per fini professionali (in relazione , ovviamente alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti;
3. debbono essere prontamente segnalati all'Azienda il furto, danneggiamento o smarrimento di tali strumenti o parti di essi con relativa denuncia alle autorità di Pubblica Sicurezza;

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni.

4.5.1 Utilizzo del personal computer

Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Responsabile del trattamento e/o dall'amministratore del sistema.

Non è consentito l'uso di programmi che non sono distribuiti ufficialmente dall'amministratore del sistema o dal Responsabile (v. in proposito, gli obblighi imposti dal D.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla L. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore);

Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

Non è consentito modificare le configurazioni impostate sul proprio PC (fermo restando la facoltà di cambiare la password assegnata, in busta sigillata, dagli uffici preposti dalla struttura ICT).

4.5.2 Utilizzo di supporti magnetici

Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus.

REGIONE LAZIO

Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163

4.5.3 Utilizzo della rete aziendale

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi.

Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

L'Azienda si riserva la facoltà di procedere alla rimozione di ogni files o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Codice di condotta.

4.5.4 Utilizzo della rete Internet e dei relativi servizi

Navigazione in Internet:

1. Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;

2. Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Responsabile o dall'amministratore del sistema e con il rispetto delle normali procedure di acquisto;

3. Non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile o dall'amministratore del sistema;

4. E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

5. Non è permessa la partecipazione, per motivi non professionali a Forum, l'utilizzo di chat line, social network, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

6. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

7. È severamente vietato aggirare le protezioni applicate dalla struttura ICT con software capace di farlo.

4.5.5 Utilizzo della Posta Elettronica

L'account di posta elettronica aziendale viene assegnato a tutti i dipendenti e collaboratori al momento dell'entrata in forze all'Azienda e viene revocato al termine del contratto di lavoro. L'account è di proprietà dell'Azienda e viene assegnato per l'attività lavorativa del dipendente o collaboratore.

L'account può essere assegnato anche a personale esterno all'Azienda e revocato qualora venga a decadere il motivo dell'assegnazione.

Il Titolare potrà accedere per motivi assolutamente connessi allo svolgimento della attività aziendale, oltre che in assenza del lavoratore, in situazioni nelle quali non si potrà in

altro modo accedere a necessarie informazioni e comunicazioni che diversamente se non ricevute ovvero recepite con ritardo potrebbero verosimilmente arrecare un evidente pregiudizio economico e non solo all'Azienda.

L'account di posta elettronica aziendale assegnato è quindi uno strumento di lavoro e per i motivi sopra esposti si ritiene utile segnalare che:

1. non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;

2. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, ecc.;

3. la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare dati sensibili se non previa crittografia;

4. ogni comunicazione (interna ed esterna), inviata o ricevuta, che abbia contenuti rilevanti o contenga dati sensibili, deve essere autorizzata dal Responsabile o dal Titolare del Trattamento, mentre per ogni altra comunicazione di carattere ordinario, interna ed esterna, si deve fare riferimento alle procedure in essere per tale corrispondenza;

5. non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale assegnato per la partecipazione a dibattiti (interni ed esterni), Forum, mail-list, salvo diversa ed esplicita autorizzazione del Responsabile o del Titolare;

6. non è consentito utilizzare l'account di posta elettronica aziendale per l'iscrizione a siti non attinenti alla propria attività lavorativa;

7. è sconsigliato l'invio di messaggi e-mail con allegati molto grandi verso molti utenti ovvero utilizzare lo strumento di posta elettronica in maniera non appropriata causando danni all'intero sistema (ad esempio l'invio di una e-mail a 100 utenti con un allegato di 20MB). Qualora si dovesse rendere necessaria la condivisione di file molto grandi verso molti utenti sarà necessario procedere alla pubblicazione del materiale sul portale aziendale, strumento più appropriato per tali comunicazioni.

L'Azienda ha messo a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (ad esempio, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro incaricato o altre utili modalità di contatto della struttura. È quindi opportuno che l'incaricato si avvalga di tali funzione, per prevenire così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora l'incaricato non possa attivare la procedura descritta, il Titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, il responsabile per la protezione dei dati), l'attivazione di un analogo accorgimento.

La procedura per l'attivazione della risposta automatica (funzione chiamata a volte *fuori sede*) è descritta nel Manuale OWA disponibile nel portale nella sezione Documentazione/Posta Elettronica.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei

messaggi di posta elettronica, l'interessato può delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il Titolare si riserva comunque di accedere all'account di posta elettronica assegnata all'incaricato nei casi in cui il protocollo incaricato/fiduciario non permetta di accedere alla posta elettronica dell'incaricato in situazioni particolari ad esempio qualora il fiduciario designato non accetti l'incarico o in caso di assenze a catena dell'incaricato e del fiduciario. A cura del Titolare o del Responsabile del trattamento, di tale attività verrà redatto apposito verbale e informato l'incaricato interessato alla prima occasione utile.

Nei messaggi di posta elettronica è bene che l'incaricato inserisca un avvertimento ai destinatari nel quale dichiari l'eventuale natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza dell'incaricato.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, gli uffici incaricati verificheranno, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

4.5.6 Registrazione accessi

Per motivi di sicurezza tutti gli accessi a internet e alla posta elettronica sono sottoposti a registrazione degli accessi (log). I log vengono mantenuti per 7 giorni solo per verifiche inerenti la sicurezza dei sistemi informatici. Solo gli amministratori dei firewall e della posta elettronica possono, previa autorizzazione scritta da parte della direzione ICT, accedere ai log.

Nei log sono presenti le seguenti informazioni:

- postazione di lavoro dal quale l'utente effettua l'accesso;
- data e ora di accesso;
- siti internet richiesti;
- nome utente;
- mittente e destinatario di posta elettronica;
- oggetto della mail.

Non vengono effettuati backup dei log della navigazione internet e dei log della posta elettronica.

REGIONE LAZIO
Azienda Ospedaliera "Complesso Ospedaliero San Giovanni Addolorata"
Via dell'Amba Aradam, 9 - 00184 ROMA - Tel. (06) 77051-Fax 77053253 - C.F. e P.IVA 04735061006 - Cod. Attività 8511.2
L.R. Lazio 16.06.94, n.18 - D.G.R. Lazio 30.06.94, n.5163