

LA GESTIONE DEI DATI NELLO STUDIO MEDICO DI MEDICINA GENERALE E PEDIATRI DI LIBERA SCELTA  
Piccolo manuale operativo con formule per le lettere di incarico e formazione del personale

06/04/2009

Avv. Paola Ferrari – info@studiolegaleferrari.it- www.studiolegaleferrari.it  
Via G. Carducci, 1/f Cassina De Pecchi – 02 9522003

## SOMMARIO

LE REGOLE IN SINTESI .....	3
RACCOLTA CONSENSO ED ESPOSIZIONE DELLE INFORMATIVE .....	3
RISERVATEZZA NELLA FASE DI ACCETTAZIONE DEL PAZIENTE E PRENOTAZIONE VISITA .....	4
L'USO DEL TELEFONO .....	4
PROCEDURE PER IL RITIRO DEI REFERTI E RICETTE .....	5
MISURE DI SICUREZZA INFORMATICA E DOCUMENTO PROGRAMMATICO.....	5
LE LETTERE DI INCARICO.....	7
Bozza lettera di incarico .....	7
Bozza lettera incarico all'amministratore di sistema .....	8
LA FORMAZIONE DEL PERSONALE E LE REGOLE DA RISPETTARE.....	8
Esempio regolamento del personale.....	9

## LE REGOLE IN SINTESI

Nella newsletter N. 17 del 19 Dicembre 2008, il Garante per la protezione dei dati è intervenuto nuovamente per esortare i medici al rispetto della normativa in materia di trattamento dei dati

In più di un' occasione prima di allora , il Garante era intervenuto poi presso medici di base ricordando loro la necessità di adottare cautele durante i colloqui con i pazienti e nella gestione delle ricette e referti.

E' opportuno, quindi, ricordare ai medici alcune semplici regole da adottare nella gestione quotidiana del lavoro.

Ecco in sintesi le procedure da seguire :

- ✓ Informativa e consenso sia come obbligo che come manifestazione di rispetto delle persone
- ✓ Le prescrizioni mediche, referti e documenti contenenti dati sanitari devono essere consegnate solo al paziente o ritirate anche da persone diverse sulla base di una delega scritta mediante la consegna in busta chiusa.
- ✓ Il medico dovrà prestare molta cura alla formazione del personale, sia nella fase di accoglienza del paziente che in quello successivo piu' propriamente amministrativo di consegna del referto e/o della ricetta.
- ✓ Redazione del documento programmatico quale momento di riflessione, lettere di incarico e formazione degli incaricati
- ✓ Avere massima cura dei sistemi informatici e delle misure di sicurezza per la loro protezione
- ✓ E' quindi necessario ricordare in pochi punti quali sono gli obblighi che i medici di medicina generale devono assolutamente rispettare.

## RACCOLTA CONSENSO ED ESPOSIZIONE DELLE INFORMATIVE

Ricordarsi, all'atto dell'apertura della scheda sanitaria di raccogliere il consenso al trattamento dei dati .

**E' opportuno esporre l'informativa in sala d'aspetto ed in particolare nelle vicinanze dei punti di accoglienza.**

### INFORMATIVA

### MEDICO

Garante 19 luglio 2006 (G.U. n.183 del 8 agosto 2006)

- desidero informarvi che i vostri dati sono utilizzati solo per svolgere attività necessarie per prevenzione, diagnosi, cura, riabilitazione o per altre prestazioni da voi richieste, farmaceutiche e specialistiche.
- si tratta dei dati forniti da voi stessi o che sono acquisiti altrove, ma con il vostro consenso, ad esempio in caso di ricovero o di risultati di esami clinici.
- anche in caso di uso di computer, adotto misure di protezione per garantire la conservazione e l'uso corretto dei dati anche da parte dei miei collaboratori, nel rispetto del segreto professionale. sono tenuti a queste cautele anche i professionisti (il sostituto, il farmacista, lo specialista) e le strutture che possono conoscerli.
- i dati non sono comunicati a terzi, tranne quando sia necessario o previsto dalla legge.
- si possono fornire informazioni sullo stato di salute a familiari e conoscenti solo su vostra indicazione.
- in qualunque momento potrete conoscere i dati che vi riguardano, sapere come sono stati acquisiti, verificare se sono esatti, completi, aggiornati e ben custoditi, e far valere i vostri diritti al riguardo.
- per attività più delicate da svolgere nel vostro interesse, sarà mia cura informarvi in modo più preciso.

Il consenso può essere raccolto anche una sola volta.

**I medici possono raccogliere il consenso anche verbalmente ma si consiglia di limitare questa prassi a casi particolari e non come normale procedura di lavoro.**

## RISERVATEZZA NELLA FASE DI ACCETTAZIONE DEL PAZIENTE E PRENOTAZIONE VISITA

Il personale deve essere istruito ad evitare di conversare con i pazienti del loro stato di salute ed in particolare delle loro patologie.

La prenotazione e le visite devono avvenire con modalità tali da evitare che altri pazienti possano sentire le conversazioni e/o individuare l'interlocutore.

### COMUNICAZIONI

- IN PRESENZA DI ALTRI PAZIENTI E/O TERZI IN SALA ATTESA, L'OPERATORE SANITARIO DOVRA' **USARE L'ACCORTEZZA DI NON COMUNICARE ALL'ACCETTAZIONE GLI ESITI E/O LA NECESSITÀ DI ULTERIORI ACCERTAMENTI A VOCE ALTA.**

## L'USO DEL TELEFONO



**PER NESSUN  
MOTIVO DOVRANNO  
ESSERE COMUNICATE  
PATOLOGIE  
TELEFONICAMENTE**

05/04/2009


## PROCEDURE PER IL RITIRO DEI REFERTI E RICETTE

Il garante ha piu' volte sanzionato i medici di medicina generale che abbandonavano le ricette dei pazienti in ambulatorio e nelle sale d'attesa o le consegnavano a persone non autorizzate.

E' importante, quindi seguire alcune semplici regole per evitare di incorrere in gravi sanzioni e/o peggio in contestazioni da parte dei pazienti.

E' necessario evitare di comunicare diagnosi a persone diverse dall'interessato, soprattutto per telefono .

**CONSEGNA RICETTE**



- **DEVONO ESSERE INSERITE IN BUSTE CHIUSE E SIGILLATE**
- **NON DEVONO ESSERE LASCIATE IN SALA D'ASPETTO**
- **PROGRAMMARE ORARI PER IL RITIRO DELLE RICETTE ( ES. INIZIO            AMBULATORIO/FINE AMBULATORIO)**

12/04/2009

## MISURE DI SICUREZZA INFORMATICA E DOCUMENTO PROGRAMMATICO

I medici vivono l'obbligo della redazione del documento programmatico della sicurezza dei dati come una "scocciatura" annuale.

**La procedura deve essere svolta entro il 31 marzo di ogni anno.**

Il documento programmatico della sicurezza, quindi, è considerato dalla legge quale una "misura minima di sicurezza"( ART. 34, lettera g) , ed integra oltre che un possibile profilo di responsabilità civile nel caso di perdita e/o uso non conforme di dati con danneggiamento di terzi, un reato penalmente sanzionato dall'art. 169 del codice .

Al contrario deve essere considerato un momento importante per analizzare con attenzione le misure di sicurezza ed i sistemi che vengono adottati per proteggere i dati dei pazienti . La ragione è logica...

- ✓ Com'è possibile che esista sicurezza senza una analisi dei rischi ed un piano per fronteggiarli?
- ✓ Com'è possibile garantire la sicurezza senza che il personale venga adeguatamente formato?

E' necessario ricordare che i dati contenuti nel proprio sistema informatico costituiscono un valore inestimabile, la perdita vorrebbe dire ricostruire archivi e perdere informazioni.


Come si chiude la porta di casa prima d'uscire è fondamentale mettere in salvo i propri dati ed il proprio lavoro prima di uscire dallo studio.

E' importante quindi, seguire alcune semplici regole:

- ✓ Dati crittografati, utilizzate uno dei programmi specifici per la gestione della cartella clinica avendo cura, scegliendo il prodotto, di verificare che sia adeguatamente protetto
- ✓ Cambiate le passwords di accesso almeno ogni tre mesi

## LE PASSWORDS

- LE CREDENZIALI E LE PASSWORDS ASSEGNATE SONO PERSONALI E NON CEDIBILI .
- SCEGLIETE PAROLE FORMATE DA NUMERI E LETTERE, DI NON MENO DI 8 CARATTERI
- DEVONO ESSERE CAMBIATE OGNI 3 MESI



12/04/2009

- ✓ Proteggete le vostre passwords

## RISERVATEZZA

NON ATTACCARE BIGLIETTI CON LE  
PASSWORD SUI MONITOR O IN  
LUOGHI ACCESSIBILI A TERZI



12/04/2009

- ✓ Fate regolari e giornalieri back up dei dati
- ✓ Tenete le copie dei dati in luogo diverso da quello dove risiede il personal computer

## PROTEZIONE DEI DATI



- FARE IL BACK-UP DEI DATI ALMENO UNA VOLTA ALLA SETTIMANA MEGLIO OGNI GIORNO
- VERIFICARE SPESSO DI ESSERE IN GRADO DI RIPRISTINARE I DATI SALVATI

a cura di COSI srl e avv. Paola Ferrari

- ✓ Proteggete il sistema con un sistema antivirus e firewall anche se non collegati ad internet, i virus possono essere annidati anche in file contenuti in altri documenti
- ✓ Fate inibire fin dall'origine alcuni siti a piu' alto rischio di spamming ( es. social network, facebook, secondlife, siti e-commerce e/o ludici).

- ✓ Utilizzate personale specializzato per la manutenzione sottoscrivendo un contratto che obblighi il consulente al rispetto delle normative ed obbligandoli al rispetto delle piu' scrupolose regole di manutenzione.

**COME PROTEGGERSI** 

- **UTILIZZARE UN ANTIVIRUS:**
  - AGGIORNAMENTI AUTOMATICI
  - SCANSIONI PROGRAMMATE
  - PROTEZIONE FILE SYSTEM & E-MAIL
  
- **UTILIZZARE UN ANTI-SPYWARE**
  - AGGIORNAMENTI AUTOMATICI
  - SCANSIONI PROGRAMMATE

a cura di COSI srl e avv. Paola Ferrari

## LE LETTERE DI INCARICO

Non esiste consapevolezza senza formazione. Il medico dovrà responsabilizzare il personale ed altri collaboratori come i medici sostituti.

La lettera d'incarico, oltre ad essere obbligatoria è anche un sistema per obbligare i terzi alla massima responsabilità.

---

## BOZZA LETTERA DI INCARICO

Il sottoscritto dott..... in qualità di Titolare/Responsabile del trattamento dei dati

### INCARICA

..... (inserire dati anagrafici: nato il ..... a .....) al trattamento dei dati sensibili, sanitari ed amministrativi nonché nell'ambito delle funzioni di ..... A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali e sensibili devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta e per la gestione della corretta manutenzione delle cartelle cliniche e dati conseguenti;
- è necessaria la verifica costante dei dati ed il loro aggiornamento, non è ammessa cancellazione non autorizzata;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile in generale ed elencate nel d.p.s.

Per ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:

- a) divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;
- b) l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
- c) la fase di trattamento dei dati dovrà essere preceduta dalla informativa al paziente in forma scritta e dal consenso di quest'ultimo al trattamento nei casi previsti dalla legge;
- d) in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;

e) le proprie credenziali di autenticazione sono strettamente personali e devono rimanere riservate. Tali credenziali sono elencate nel documento programmatico sulla sicurezza dell'Associazione e univocamente associate all'incaricato al quale sono state fornite.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Qualsiasi altra istruzione può essere fornita dal Titolare che provvede anche alla formazione degli incaricati.

Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottato dall'Associazione.

#### TRATTAMENTO CONSENTITO

a) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli cartacei e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

b) qualsiasi accesso e trattamento espressamente previsto dal profilo di autorizzazione associato e descritto nel D.p.s.;

c) qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Data \_\_\_\_\_

L'incaricato FIRMA

---

#### BOZZA LETTERA INCARICO ALL'AMMINISTRATORE DI SISTEMA

Conformemente a quanto stabilito dal D.lgs196 /2003 affido al sig. /soc ..... l'incarico di Amministratore di Sistema per tutti gli elaboratori in uso presso la società .

E' compito degli "Amministratori di Sistema":

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up e di disaster recovery secondo i criteri stabiliti dal "Responsabile del trattamento per la sicurezza dei dati";
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- Fare in modo che sia prevista la disattivazione dei "codici identificati personali" (User-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel
- caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per oltre 6 mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

L'"Amministratore di sistema" dichiara di essere a conoscenza di quanto stabilito dal DPR 318 del 28 luglio 1999 nonché dal D. Lgs. 196 /2003 e delle indicazioni contenute nel Documento Programmatico della Sicurezza dei dati applicato presso l'Associazione.

Si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte nonché dalle eventuali successive normative in materia.

#### LA FORMAZIONE DEL PERSONALE E LE REGOLE DA RISPETTARE

Il personale deve essere responsabilizzato alla corretta gestione e manutenzione dei sistemi informatici.

Spesso il personale, anche il più efficiente, utilizza internet e la posta elettronica. Facile quindi che utilizzi i sistemi anche per ragioni personali.

E' opportuno, quindi, che oltre alla lettera di incarico sia fornita una adeguata nota di istruzioni in modo che sia possibile anche procedere disciplinarmente in caso di violazioni.

E' importante, quindi, provvedere con adeguate istruzioni scritte.

## ESEMPIO REGOLAMENTO DEL PERSONALE

### OGGETTO

Il presente regolamento, valido ed efficace anche ai fini disciplinari ai sensi dell'art. 7 della legge 30/05/1970 n. 300 riguarda :

- a) le modalità di utilizzo degli strumenti informatici nell' ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e nelle attività di ufficio da parte dei dipendenti che hanno in dotazione una stazione di lavoro di tipo personal - computer o terminale;
- b) l' individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia e gli adeguati livelli di sicurezza ed integrità del patrimonio informativo.

### CAPO I

#### UTILIZZO DEGLI STRUMENTI INFORMATICI

#### MODALITÀ DI UTILIZZO DEGLI STRUMENTI INFORMATICI IN DOTAZIONE

Durante l'espletamento della propria attività lavorativa:

#### NON È CONSENTITA:

- l'installazione e la duplicazione di software non coperto da regolare licenza fornita dal Responsabile Gerarchico di appartenenza o dalla Direzione Generale;
- l'installazione di software libero non soggetto a licenza d' uso, non autorizzato dal responsabile gerarchico di appartenenza o dal Servizio Sistemi Informativi;
- l'installazione di software non autorizzato, finalizzato ad alterare la funzionalità del collegamento in rete della stazione di lavoro;
- l'alterazione degli indirizzi e dei protocolli di rete assegnati dal Servizio Sistemi

Informativi;

- la spedizione e la ricezione, via e-mail Internet, di messaggi o archivi per usi non diversi dalle mansioni ricoperte , comunque non inerenti i propri compiti di ufficio, mettendo così a rischio la sicurezza e l'integrità del patrimonio informativo;
- l'inibizione o la sospensione, anche temporanea, del funzionamento del software ANTIVIRUS installato;
- l'utilizzazione di funzioni e tecniche di condivisione dei propri archivi senza la contemporanea adozione di opportune parole chiave di accesso da fornire ai colleghi che ne debbano fare uso;
- l'apertura di canali informativi telematici non autorizzati, da e verso l'esterno alla in qualsiasi forma (trasferimento dischetti, modem, Internet, ecc.).

#### È OBBLIGATORIA:

- l'utilizzazione di tutte le cautele riguardanti l'uso di software del quale non si conoscano appieno le potenzialità;
- l'attività di aggiornamento del proprio software ANTIVIRUS ogni qualvolta ne venga

indicata o ravvisata la necessità;

La comunicazione al responsabile gerarchico di appartenenza della eventuale parola chiave (hardware) utilizzata per accedere alla propria stazione di lavoro. Il Settore/Servizio/ Ufficio è tenuto a custodire l'archivio delle parole chiavi aggiornato, necessario per intervenire in caso di emergenza. Senza tale parola chiave il computer diviene INUTILIZZABILE.

la comunicazione al responsabile gerarchico di appartenenza dell'insorgere di condizioni anomale che possono comportare una non perfetta aderenza alle norme di

comportamento indicate nel presente regolamento.

## ACCESSO AI SITI INTERNET

E' vietato l'accesso a siti Internet diversi da quelli pubblici e/o assolutamente necessari per far fronte alle mansioni assegnate-

E' vietato l'uso di siti e-commerce se non espressamente autorizzati per ragioni del proprio servizio è altresì vietato l'accesso e la navigazione in siti immorali, pedofili, pornografici, ludici, musicali e, comunque a qualsiasi sito non espressamente autorizzato.

La violazione della presente norma autorizzerà, a seconda della gravità della violazione, alla massima disposizione disciplinare prevista dal contratto collettivo di lavoro e, nei casi più gravi potrebbe determinare anche l'immediato licenziamento.

## CAPO II

### MISURE DI SICUREZZA PER LA TUTELA DEI DATI

#### CODICI IDENTIFICATIVI E PROTEZIONE DEGLI ELABORATORI

Nel caso di trattamenti effettuati con gli elaboratori:

- a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempidiversi, essere assegnato a persone diverse;
- b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi e tre per quei settori che trattano dati sensibili;
- c) gli elaboratori devono essere protetti contro il rischio di intrusione mediante idonei programmi antivirus, la cui efficacia ed aggiornamento sono verificati con cadenza almeno trimestrale.

#### ACCESSO AI DATI PARTICOLARI

Per il trattamento dei dati sensibili o/e giudiziari l'accesso per effettuare operazioni è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento.

Se il trattamento è effettuato con elaboratori accessibili mediante una rete di telecomunicazioni disponibile al pubblico, sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione.

L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare, o dal responsabile.

Periodicamente, e comunque almeno semestralmente, è verificata la sussistenza delle condizioni per la loro conservazione.

L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento.

La validità delle richieste di accesso è verificata prima di consentire l'accesso stesso.

Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

I dati sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità.

I dati sono conservati, separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. Al trattamento di tali dati si procede con le modalità di cui al comma precedente anche quando detti dati non sono contenuti in elenchi, registri o banche dati o non sono tenuti con l'ausilio di mezzi elettronici o comunque automatizzati.

Rispetto ai dati la cui disponibilità è essenziale per svolgere attività istituzionali le operazioni di trattamento autorizzate sono quelle strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.

#### DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Nel caso di trattamento dei dati sensibili e/o giudiziari effettuato mediante gli elaboratori deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

- a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
- b) i criteri e le procedure per assicurare l'integrità dei dati;
- c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
- d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni;

L'efficacia delle misure di sicurezza deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Nel caso di trattamento dei dati sensibili e/o giudiziari, il reimpiego dei supporti di memorizzazione già utilizzati per il trattamento può essere effettuato qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

#### TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI.

Nel caso di trattamento di dati personali, effettuato con strumenti diversi, sono osservate le seguenti modalità:

- a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni il titolare o il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato definendo procedure di consegna e restituzione dei documenti.

Nel caso di trattamento di dati sensibili e/o giudiziari, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:

- a) Gli atti e i documenti contenenti i dati sono conservati in luoghi chiusi, sale contenitori muniti di serratura;
- b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

#### CAPO III

##### DISPOSIZIONI FINALI

##### COMPITO DI SORVEGLIANZA

I responsabili di ciascun ufficio hanno il compito di sorvegliare il corretto rispetto delle modalità di utilizzo degli strumenti informatici in dotazione ai dipendenti, nonché di disporre eventuali ulteriori direttive giudicate necessarie nell'ambito di particolari specificità o responsabilità.

##### INOSSERVANZA DELLE DISPOSIZIONI

L'inosservanza delle presenti disposizioni potrà comportare conseguenze sul piano

disciplinare, civile, penale e patrimoniale.

##### DISPOSIZIONI DI RINVIO

Si fa riserva di adottare successive eventuali integrazioni o correzioni alle disposizioni del presente regolamento, in relazione all'entrata in vigore di sopravvenute normative ed all'evolversi della tecnologia.