Indice

	REVISIONI					
EDIZIONE: prima	***0***	***1***	***2***	***3***	***4***	***5***
Data	*29.04.16*					
Emessa da	*AU*					
Approvata da	*AU*					
Motivazione	*Adeguamento al D.Lgs. 231/01*					

L'Amministratore Unico

1. Scopo

Scopo del presente protocollo di **Casa di Cura Privata Nuova Villa Claudia S.p.A.** è contribuire alla creazione di un corretto sistema di regole ed accorgimenti, teso alla prevenzione dei reati informatici e di quelli previsti dal D.Lgs. 196/03.

2. Campo di applicazione

Il protocollo verrà applicato a tutti i trattamenti di dati aziendali con particolare attenzione a quelli effettuati con l'ausilio di strumenti elettronici.

3. Descrizione delle attività

Le principali attività del processo fanno riferimento alle attività di raccolta, registrazione, consultazione, elaborazione , modificazione, selezione, estrazione, raffronto, utilizzo, blocco, comunicazione, cancellazione, conservazione, organizzazione, interconnessione, distruzione, diffusione dei dati aziendali, sia in forma elettronica, che cartacea.

4. Criteri operativi

Ogni dipendente incaricato del Trattamento dei dati personali, dovrà attenersi alle disposizioni di seguito riportate:

- operare garantendo la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati personali confidenziali e segreti;
- per nessun motivo diffondere o comunicare a terzi dati personali, ad eccezione dei soggetti ed entità previsti dalla società per l'adempimento degli scopi previsti;
- non consegnare o duplicare dati personali per finalità diverse da quelle della mansione assegnata;
- evitare che i dati personali possano essere soggetti a rischi di perdita o distruzione anche accidentale, che ai dati possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati sono stati raccolti e per i quali vengono trattati;
- operare solo ed esclusivamente nell'ambito del proprio profilo professionale assegnato dal Titolare o Responsabile del trattamento;

- restituire integralmente al Titolare i dati personali in possesso, dopo l'eventuale cessazione del rapporto di lavoro dipendente in essere o di cambiamento della mansione;
- osservare le disposizioni emanate dalla società in materia di sicurezza e riservatezza; custodire e controllare i dati personali mediante l'adozione delle misure di sicurezza previste per evitarne la distruzione, la perdita e l'accesso da parte di terzi;
- conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- in caso di trattamenti dei dati personali che richiedano l'uso di sistemi informatici e telematici, gestire la propria password secondo le indicazioni del Titolare o Responsabile del trattamento conformemente alle indicazioni del D.lgs. 196/03 e del disciplinare tecnico allegato sub b).

SI RIPORTA DI SEGUITO IL REGOLAMENTO (A CUI OGNI INCARICATO DOVRÀ ATTENERSI) PREVISTO DALL'AMMINISTRATORE UNICO RIGUARDANTE LA GESTIONE INFORMATIZZATA E CARTACEA DEI DATI:

Utilizzo del personal computer

Il Personal Computer affidato al dipendente deve essere da lui utilizzato solo ed esclusivamente per svolgere l'attività lavorativa. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare o Responsabile del Trattamento.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare o Responsabile del Trattamento, in quanto sussiste il grave

pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare o Responsabile del Trattamento.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare o Responsabile del Trattamento

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Titolare o Responsabile del Trattamento.

Ogni utente deve avvertire immediatamente il Titolare o Responsabile del Trattamento nel caso in cui vengano rilevati virus.

<u>Utilizzo della rete</u>

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. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente. Il Titolare o Responsabile del Trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto

grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Gestione delle password

Il trattamento elettronico dei dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione consistente nell'inserimento di un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata creata e conosciuta esclusivamente dallo stesso.

Ogni codice di identificazione è utilizzato da un solo incaricato e non è assegnato ad altri.

Le password sono riservate e conosciute esclusivamente dall'incaricato, che deve assicurarne anche la riservatezza. A tal fine gli incaricati ricevono apposite istruzioni (vedi appendice). La lunghezza minima delle password, che non contengono riferimenti agevolmente riconducibili all'incaricato, è di otto caratteri ovvero quella massima consentita dal software gestionale aziendale.

Le password vengono modificate al primo utilizzo e periodicamente ogni tre mesi in caso di trattamento dei dati sensibili ed ogni sei mesi per tutti gli altri trattamenti di dati.

Il Titolare o Responsabile del Trattamento provvede a revocare tutte le password non utilizzate per un periodo superiore a 6 mesi, nonché quelle appartenenti al personale che abbia perso la qualità di incaricato.

Il Titolare o Responsabile del Trattamento predisporrà (personalmente o delegando il compito ad un incaricato che provvederà a nominare custode delle password) tante buste chiuse quanti sono gli incaricati al trattamento. Tali buste, riconoscibili all'esterno dal nome dell'incaricato, conterranno le password generate dagli incaricati e dovranno essere custodite in un posto sicuro e non accessibile. Qualora la compagine degli incaricati dovesse variare, il Custode provvederà a distruggere le relative buste ed eventualmente, se necessario, a predisporne delle nuove per i nuovi incaricati ricordandosi sempre che una parola chiave già utilizzata non può essere riassegnata ad un nuovo utente. Il procedimento fin qui descritto deve essere effettuato anche in presenza di un solo PC.

Al fine di procedere ad una corretta scelta della password è consigliabile tener presente che la parola chiave non deve essere:

Un nome proprio, nome di animali, nomi di parenti o colleghi, nomi di città o nazioni, date di nascita, numeri di telefono, la data di una ricorrenza, una password nuova che abbia una minima differenza con la precedente, una parola comune (es.: casa, auto, moto, ecc.), una sequenza alfabetica o numerica (es.. 12345, abcde).

Al fine di conciliare l'esigenza di garantire una buon livello di sicurezza alla parola chiave con quella di agevolare una semplice memorizzazione, si può procedere a: creazione di un acronimo, consistente in una sigla composta dalle iniziali di una frase (es.: sopra la panca la capra campa sotto

la panca la capra crepa - SLPLCCSLPLCC), creazione di una parola priva di senso composta dalle prime quattro lettere di due parole (es.: vagone ferroviario - VAGOFERR), codice alfanumerico costituito da una parte di parola ed un numero (es.: tempesta 73 - TEMPES73), creazione di una parola priva di senso inserendo all'interno di una parola un numero od una lettera a caso (es.: granita - graPnita), creazione di una parola priva di senso utilizzando caratteri speciali (es.: marmellata - M@RMELL@T@, spavaldo - $P@V@LDO ecc.).

Le password devono essere conservate osservando scrupolosamente le seguenti indicazioni:

non devono essere mai rivelate a nessuno, non devono essere mai annotate su foglietti di carta o sulle agende, non devono essere mai riutilizzate o recuperate tra quelle vecchie, non devono mai essere riportati sul presente documento o su moduli o procedure, non devono essere mai rivelate al telefono, non devono essere mai rivelate in messaggio di posta elettronica o in un SMS, non devono essere mai rivelate ad un collega di lavoro, neanche in previsione di un'assenza prolungata dovuta a vacanze o maternità.

La direzione può prevedere azioni disciplinari di vario livello verso l'incaricato che abbia violato le disposizioni impartite, mettendo a rischio il trattamento dei dati personali.

Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico).

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal titolare responsabile del trattamento e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.

Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, deve essere utilizzata esclusivamente per l'effettuazione delle comunicazioni inerenti l'attività lavorativa. Le persone assegnatarie delle

caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'azienda deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno dell'azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al responsabile o titolare del trattamento. Non si devono in alcun caso attivare gli allegati di tali messaggi.

<u>Uso della rete internet e dei relativi servizi</u>

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Titolare o Responsabile del Trattamento.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
È severamente vietato l'accesso a siti pornografici, con particolare riguardo a quelli che potrebbero contenere immagini e filmati con coinvolgimento di minori.

Osservanza delle disposizioni in materia di privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.Lgs. n. 196/2003.

Non osservanza della normativa aziendale

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Gestione documentazione cartacea e monitor

Bisogna accuratamente evitare che i documenti contenenti dati personali siano lasciati per un tempo indeterminato liberi ed incustoditi per i locali aziendali; occorre invece che gli incaricati, a cui essi sono affidati per lo svolgimento delle loro mansioni, provvedano a controllarli e custodirli, per poi riporli negli appositi schedari al termine delle operazioni di loro competenza.

Va prestata quindi attenzione affinché tutti i documenti cartacei contenenti dati personali (soprattutto in presenza di clienti) non si trovino sparsi su scrivanie, ripiani o in luoghi in cui siano visibili a terzi non autorizzati, che possono venirne a conoscenza e divulgarli.

Simili accorgimenti vanno poi adottati dagli incaricati che effettuano il trattamento elettronico dei dati personali, che, soprattutto nei luoghi in cui è possibile il passaggio o la permanenza dei clienti, devono, in caso di momentaneo allontanamento dalle loro postazioni, rendere temporaneamente inaccessibili e non leggibili le informazioni presenti sul video (anche uscendo dal programma).

Il Referente è il Responsabile Area Tecnica e Servizi di Supporto, con la collaborazione del Responsabile del trattamento.

Il Responsabile Area Tecnica e Servizi di Supporto informa l'Organismo di Vigilanza, con

frequenza definita dalla tabella flussi informativi, attraverso uno specifico report (Mod. 18) in merito:

- ai controlli effettuati;
- agli eventuali rilievi e/o difformità riscontrati nel corso dei controlli.

Il Responsabile di funzione deve informare tempestivamente e senza indugio l'Organismo di Vigilanza in ordine ad eventuali comportamenti a rischio reato 231 inerenti i processi operativi di propria competenza, di cui sia venuta a conoscenza in via diretta o per il tramite di informativa ricevuta dai propri collaboratori.