studiofarma SOFTWARE & SOLUTIONS

una società di CGM CompuGroup Medical

Alla C.A.

Tutti gli Ordini dei Farmacisti utilizzanti i servizi

OrdineP-NET

Brescia, 21 Ottobre 2015

Oggetto: **Aggiornamento del Documento Programmatico sulla Sicurezza anno 2015 e adempimenti in tema di Amministratori di Sistema relativi all'applicazione OrdineP-Net**

Gentile Cliente,

le comunichiamo gli adempimenti intrapresi da codesta Società al fine di dar corso alle specifiche previsioni normative ex D. Lgs. 196/2003, riguardo ai trattamenti di dati personali effettuati mediante OrdineP-Net .

1) **Misure di sicurezza, sia minime che idonee, ed azioni adottate per la messa in protezione dei dati gestiti**

Tutti i documenti cartacei contenenti dati personali sono conservati presso le sedi di Studiofarma o presso i locali di soggetti esterni che sono stati nominati quali Responsabili del trattamento.

Tutti gli accessi alle banche-dati utilizzate sono registrati presso il server dove sono residenti tali banche-dati.

I dati trattati persistono su strutture diversificate per separare i dati comuni dai dati sensibili; il ricongiungimento è possibile solo con chiavi numeriche non parlanti.

L'accesso ai database è gestito dal sistema informatico tramite il "sistema di autenticazione": nome utente abbinato ad una password di almeno 8 caratteri, la password viene modificata almeno ogni tre mesi.

Tutti i trattamenti sono effettuati presso la sede di Studiofarma o CompuGroup Medical (CGM) mediante l'utilizzo di personal computer o computer portatili; nel caso dell'utilizzo di personal computer o computer portatili, fuori dai locali indicati, l'accesso ai suddetti dati è consentito previo accesso securizzato ad una VPN aziendale.

Gli Incaricati sono stati informati che qualora fosse necessario archiviare dati personali su supporti rimuovibili, tali supporti andranno custoditi con la necessaria diligenza al fine di non mettere in pericolo (distruzione, dispersione, sottrazione ...) i dati in essi contenuti; gli Incaricati sono stati altresì resi edotti che qualora tali supporti non venissero più utilizzati, il loro contenuto andrà reso inutilizzato, salvo che sia necessario per altri trattamenti autorizzati.

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano sotto la sorveglianza di Incaricati di Studiofarma.

L'Incaricato effettua la stampa dei dati solo se strettamente necessaria e la ritira immediatamente dai vassoi delle stampanti comuni.

Autenticazione informatica

Gli Incaricati ai trattamenti sono preventivamente informati per iscritto dei loro doveri in termini di riservatezza sui dati trattati e sulle misure minime di sicurezza da adottare. Queste disposizioni sono fornite loro nella lettera di nomina quali incaricati al trattamento.

Gli Incaricati sono resi edotti sul fatto che i computer non vanno mai lasciati accessibili a soggetti terzi quando sono incustoditi; quindi è obbligatorio bloccare forzatamente il PC oppure impostare l'attivazione automatica dello *screen saver* ogni qualvolta lo si lasci incustodito, anche per breve tempo. Al riavvio dovrà essere richiesta la password (che sarà la stessa utilizzata all'accesso). In caso di attivazione automatica, lo *screen saver* deve essere programmato per attivarsi in un tempo ragionevole e compatibile con l'attività lavorativa, e comunque il più breve possibile (per il personale di Studiofarma e CGM questo viene effettuato automaticamente ogni 10-15 minuti di inattività).

L'accesso al computer, sia esso in rete o meno, è sempre protetto da una procedura di autenticazione informatica.

Agli Incaricati ed ai soggetti autorizzati, che accedono alle banche dati gestite con strumenti informatici, è assegnato un codice identificativo personale univoco, non cedibile ed immodificabile, il cui corretto utilizzo è regolamentato con apposita comunicazione. Gli incaricati ed i soggetti autorizzati devono dotarsi di una password riservata, composta da almeno 8 caratteri. Le password devono essere modificate al primo utilizzo e successivamente almeno ogni 3 mesi.

Gli account attribuiti ad Incaricati cui è stato revocato l'incarico vengono disattivati all'atto della revoca.

Sistema di protezione contro accessi abusivi

L'hardware di protezione firewall in uso protegge tutta la rete dalle varie tipologie di programmi nocivi, compresi gli spyware; il servizio di abbonamento sottoscritto con il produttore dell'antivirus consente di recepire quotidianamente in automatico gli aggiornamenti tramite un sistema centralizzato, il quale provvede poi a sua volta ad aggiornare, sempre in modalità automatica, tutti i server interessati.

La rete informatica è protetta da sistemi anti-intrusione ridondati che impediscono accessi remoti non autorizzati ai server con servizi di Firewall & IPS (Intrusion Prevention System); Studiofarma ha sottoscritto un servizio di abbonamento con il produttore per il recepimento degli aggiornamenti dei sistemi di sicurezza.

Gli accessi degli incaricati avvengono unicamente con collegamenti cifrati (VPN).

Tutti i collegamenti con l'esterno (navigazione internet, e-mail, VPN e collegamenti WAN) sono gestiti a livello generale di rete da apparecchiature apposite (router, firewall/VPN), in modo da garantire la massima sicurezza e protezione dei dati, anche da tentativi di intrusione provenienti dall'esterno.

Nel caso di utilizzo di modem (es. PC portatili) è attivo il firewall software di Windows.

Aggiornamento dei programmi

Tutti i sistemi (server, client e antintrusione) vengono aggiornati con le ultime *patches (security hotfixes)* rilasciate dai produttori con operazioni manuali, su base trimestrale; eventuali *patches* critiche vengono applicate entro 30 gg.

Quando un determinato sistema non è più in manutenzione da parte del produttore, che si tratti di server, di PC, o di strumenti analoghi, si provvede alla sostituzione integrale (hardware e software) dell'apparecchiatura interessata.

Salvataggio dei dati su supporti di sicurezza (Backup dati)

Backup banche dati

Viene utilizzato un software di backup che esegue backup quotidiani "a caldo" in base alle seguenti regole:

- un full backup quotidiano;
- backup incrementali ogni 30 minuti durante gli orari lavorativi;
- retention: 3 giorni.

Il software di backup esegue la sincronia ed il consolidamento automatico dei dati, se il backup fallisce viene mantenuta l'ultima copia valida e viene informato l'amministratore di sistema.

I backup vengono eseguiti su Storage System forniti dal servizio I.NET-BT Data Backup tramite rete di back-end separata e dedicata.

I dati presenti in locale sui portatili sono giornalmente salvati sul server se il PC è connesso alla rete aziendale negli orari definiti per il backup. Nel caso in cui il portatile non si connetta alla rete per più di una settimana, l'utilizzatore è invitato a fare, almeno settimanalmente, il backup dei dati presenti in locale su supporti magnetici in completa autonomia (es. CD ROM, chiavi USB, ecc.) ed a conservare tali supporti in maniera tale che i dati personali contenuti in tali supporti non possano essere carpiti da soggetti estranei.

Backup server

Il software di backup esegue esegue backup quotidiani "a caldo" in base alle seguenti regole:

- Server Database: settimanale;
- Server Web/Applicativo: quotidianamente nei giorni feriali;
- Retention: 1 backup per server.

La verifica sul backup viene fatta manualmente ogni giorno feriale dall'amministratore del sistema.

I backup vengono eseguiti su storage fisici di proprietà Studiofarma.

Salvataggio (backup) degli elaboratori in cui sono presenti banche dati elettroniche

Il software di backup esegue una sincronia ed eventuale copia consolidata dei dati di servers e clients in base alle seguenti regole:

- Servers cruciali
  - Tutti i dischi dei servers a partire dalle ore 20 circa dal Lunedì al Venerdì (retention: 7 giorni)
- Clients
  - Viene eseguito il backup dei dischi essenziali dei clients (solitamente C: e D:) tra le ore 12:30 e le ore 13:30 dal Lunedì al Venerdì (retention: 1 giorno) per il personale Studiofarma

Procedure di verifica: il software di backup esegue la sincronia ed il consolidamento automatico dei dati, se il backup fallisce viene mantenuta l'ultima copia valida. La verifica viene fatta manualmente ogni giorno dall'amministratore del sistema (System Administrator)

Procedure di ripristino: viene eseguito tramite apposita procedura, selezionando il client o server interessato e successivamente quale dato si desidera ripristinare.

Ripristino della disponibilità dei dati personali, in seguito a distruzione o danneggiamento

Il tempo necessario per recuperare i dati dalle copie di sicurezza, a fronte di una generica emergenza, è al massimo di 7 giorni, a partire dal verificarsi del possibile accadimento negativo.

Le procedure di ripristino dei backup dei server sono operazioni manuali che utilizzano i tools forniti dal produttore del software di backup.

Protezione delle aree e dei locali

Gli accessi ai locali delle due sedi di Studiofarma è costantemente presidiato da personale dipendente del Titolare e l'accesso deve essere preventivamente autorizzato mediante apertura di porte chiuse a chiave.

Al di fuori dell'orario di lavoro, i locali sono protetti da impianto d'allarme collegato all'istituto di vigilanza; per la prevenzione dagli incendi, sono presenti vari estintori all'interno e nei pressi degli uffici.

I server e tutte le apparecchiature informatiche sono site negli appositi locali presso le sedi di Studiofarma e presso la *server-farm* di BT Italia S.p.A. a Settimo Milanese e/o CGM Italia a Molfetta (BA); tali locali sono correttamente climatizzati, chiusi a chiave ed accessibili solo alle persone autorizzate alle operazioni di gestione e manutenzione tecnica.

2) Elenco nominativo degli Incaricati del trattamento e degli Amministratori di Sistema, con l'assicurazione che i relativi atti sono custoditi presso la nostra sede legale

Le seguenti ulteriori persone sono state nominate - mediante atti conservati presso la Scrivente - quali Incaricati del trattamento e gli è stato indicato che, in relazione al software OrdineP, rivestono anche la qualifica di Amministratori di Sistema (così come identificata dal Provvedimento del Garante della Privacy del 27.11.2008 [doc. web n. 1577499])

Compugroup Medical Italia e Studiofarma	**EPS Italia**
o Riccardo Nauti	o Pieralberto Nati
o Andrea Borraccetti	o Daniele Fumagalli
o Angelo Curci	o Davide Gilioli
o Daniele Cuocci	o Paolo Gabbrielli

3) Rapporto sull'attività formativa erogata agli incaricati del trattamento e agli Amministratori di Sistema relativa alla disciplina ex D. Lgs. 196/2003

Annualmente presso le due sedi di Studiofarma viene svolta una riunione formativa sulla riservatezza dei dati sensibili, cui partecipano tutti gli Incaricati (compresi coloro che rivestono anche la qualità di Amministratore di Sistema ex D. Lgs. 196/2003), durante cui si procede a:

- informare gli Incaricati sul contenuto del Documento Programmatico della Sicurezza (DPS), dandone lettura;
- consegnare la lettera di incarico al trattamento dei dati;
- raccomandare sia l'osservanza di quanto contenuto nelle lettere di incarico sia di adottare la diligenza del buon padre di famiglia nel trattamento di tutti i dati personali di cui gli incaricati verranno a conoscenza;
- raccomandare di conservare tutti i documenti cartacei contenenti dati personali in locali, armadi o cassetti chiusi a chiave e custodire le chiavi con diligenza;
- raccomandare di chiudere le porte degli uffici, nel momento in cui ci si accinge ad uscire dal luogo di lavoro, e chiuderle a chiave la sera;
- invitare ogni incaricato a dotarsi di un codice di identificazione personale e di una password segreti per l'accesso ai dati personali memorizzati su strumenti elettronici;
- rammentare a ogni incaricato che la mancata osservanza delle suddette istruzioni e di quanto contenuto nella lettera di incarico può far sorgere in capo all'incaricato:
  1) responsabilità penale nei confronti di terzi per la mancata adozione delle misure minime di sicurezza;
  2) responsabilità civile nei confronti di terzi che venissero danneggiati dalla perdita, distruzione e utilizzazione illecita dei dati;
  3) responsabilità contrattuale nei confronti del datore di lavoro;

4) Rispetto delle misure previste dal Provvedimento Generale dell'Autorità garante del 27.11.2008 in materia di Amministratori di Sistema ed in particolare di quelle relative alla conservazione dei file di log e della verifica annuale del loro operato

Amministratori di Sistema

Le persone individuate annualmente quali Amministratori di Sistema (vedi punto 2 del presente documento) sono state scelte avendo riguardo all'esperienza, capacità ed affidabilità di ognuno di essi, valutando a tal fine anche il percorso di studi intrapreso, le precedenti esperienze lavorative e la frequentazione di corsi di formazione.

Registrazione accessi

Sono stati adottati idonei sistemi per la registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema, tali da garantire la completezza, inalterabilità e possibilità di verifica della loro integrità degli stessi log. I log eventi vengono conservati per sei mesi.

5) Rispetto delle misure previste dal Provvedimento Generale dell'Autorità garante del 13.10.2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche

Premesso che il contenuto del provvedimento adottato dal Garante in tema di RAEE non ha valore precettivo in quanto emanato ex art. 154, comma 1, lettera h) e non in base all'art. 154, comma 1, lettera c), comunque la scrivente precisa che tutti i supporti magnetici riutilizzabili (memorie di massa, cd, dvd, cassette e cartucce), quando cessano di essere utilizzati, vengono fisicamente distrutti; mentre quando vengono riutilizzati le informazioni in essi contenute vengono preventivamente rese inintelligibili.

6) Sedi presso le quali i dati personali sono trattati o presso le quali sono gestite e/o conservate le banche dati

I trattamenti vengono effettuati presso la sede di Studiofarma in Via Brixia Zust, 10 a Brescia (BS).

Le banche dati risiedono in server presenti nella sede suddetta, presso la Serverfarm di BT Italia localizzata in Via Darwin 85 a Settimo Milanese (MI) e nel Datacenter di Compugroup Medical Italia in via Adriano Olivetti, 10 in Molfetta (BA)

7) Conformità di OrdineP-Net alla misura 25 del Disciplinare Tecnico di cui all'Allegato B del D.Lgs. 196/2003 ossia conformità di OrdineP-Net rispetto alle disposizioni di cui al predetto Allegato B

Studiofarma attesta che OrdineP-Net è stato sviluppato e viene costantemente implementato in maniera conforme al disciplinare tecnico di cui all'Allegato B del D.Lgs. 196/2033.

8) Indicazione dell'eventuale sub-delega di attività di trattamento di dati a soggetti terzo

Non è stata concessa nessuna "sub-delega" a nessun soggetto esterno, ma si è provveduto a nominare quali Incaricati tutti i collaboratori di CompuGroup Medical, EPS Italia e Studiofarma che possono accedere alle banche dati presenti nei software OrdineP-Net .

9) Eventuale segnalazione, sulla base di un effettiva analisi, delle eventuali criticità residue nel trattamento dei dati personali, che potrebbero costituire oggetto si segnalazioni di mancato rispetto della riservatezza e dignità personale da parte dell'utenza

Dall'analisi dei rischi di seguito riportata, codesta società non evidenzia nessun profilo di potenziale residua pericolosità nel trattamento effettuato. Nella colonna "Impatto sulla sicurezza" viene riportata la gradazione della gravità di ogni rischio (Alta, Media o Bassa).

Rischio	Impatto sulla sicurezza
Comportamenti degli operatori	Bassa
sottrazione di credenziali di autenticazione;	Bassa
carenza di consapevolezza, disattenzione o incuria;	Bassa
comportamenti sleali o fraudolenti;	Bassa
errore materiale;	Bassa
Eventi relativi agli strumenti	
azione di *virus* informatici o di programmi suscettibili di recare danno;	Bassa
mail indesiderate (spam) o tecniche di sabotaggio;	Bassa
malfunzionamento, indisponibilità o degrado degli strumenti;	Bassa
accessi esterni non autorizzati;	Bassa
intercettazione di informazioni in rete;	Bassa
Eventi relativi al contesto	
accessi non autorizzati a locali o aree ad accesso ristretto;	Bassa
sottrazione di strumenti contenenti dati;	Bassa
eventi distruttivi naturali o artificiali, dolosi, accidentali o dovuti ad incuria;	Bassa
guasto a sistemi complementari (impianto elettrico, climatizzazione ...);	Media
errori umani nella gestione della sicurezza fisica.	Bassa

Rimanendo a Vostra completa disposizione per ulteriori informazioni ed eventuali chiarimenti, cogliamo l'occasione per porgerVi distinti saluti.

Studiofarma S.r.l.

Emanuele Mugnani