1. Scopo

In ottemperanza al Decreto Legislativo 231 dell'8 giugno 2001 e norme correlate in tema di responsabilità amministrativa degli enti, Farmacie Comunali S.p.a. (di seguito Società) ha predisposto il Modello di organizzazione, gestione e controllo (di seguito "Modello").

Il presente protocollo, in applicazione alle disposizioni del Modello, disciplina gli aspetti inerenti il comportamento da tenere al fine di contrastare fenomeni di criminalità informatica o similari.

L'obiettivo è pertanto quello di garantire che le attività di ICT siano svolte in modo corretto e trasparente in modo che non vi possa essere alcun spazio per attività o comportamenti che, anche indirettamente, possano potenzialmente sfociare in illeciti di criminalità informatica.

Il protocollo assolve, inoltre, il compito di agevolare il monitoraggio del processo qui descritto da parte dell'Organismo di Vigilanza.

2. Ambito di applicazione

Il presente protocollo si applica a tutte le attività che rientrano nell'ambito della Funzione sistemi informativi ed in tutte le altre funzioni o risorse aziendali quando trattano aspetti informativi ed informatici.

3. Reati da presidiare

Le attività di cui trattasi si riferiscono ai reati della Legge n. 48/2008 che ha inserito il nuovo articolo 24 bis nel Decreto 231/01. In particolare ci si riferisce ai reati e agli illeciti amministrativi per delitti informatici legati all'abuso di sistemi e al trattamento illecito di dati di cui alla Convenzione del Consiglio d'Europa sulla criminalità informatica, siglata a Budapest il 23 novembre 2001.

Si tratta quindi di prevenire e scongiurare la commissione di una serie di potenziali reati, per i quali Sono previste pene pecuniarie e interdittive molto rilevanti per la Società.

Nel caso che i reati suddetti siano commessi da personale con la qualifica di operatore di sistema informatico o telematico le pene sono aumentate.

4. Principi di prevenzione

In base alla nuova disciplina le imprese possono rispondere direttamente per una serie di delitti informatici legati all'abuso di sistemi, al trattamento illecito dei dati, mentre divengono più ampie le possibilità di perquisizioni e sequestri (ai provider potrebbe essere imposto un obbligo di conservazione dei dati telematici per un massimo di sei mesi).

La peculiarità delle condotte individuate nei reati di cui sopra è tale da ritenere marginale la loro applicazione al core business della Società, anche se a livello del tutto occasionale il potenziale verificarsi delle descritte condotte non può escludersi in assoluto.

Si precisa che nel corso delle attività di Risk Assessment è stata debitamente condotta un'analisi specifica dei processi potenzialmente a rischio dell'area dei sistemi informatici con riferimento al reato di "frode informatica", reato incluso nel novero della famiglia dei reati contro la Pubblica Amministrazione.

Inoltre la stessa area informatica è opportunamente presidiata e verificata in ottemperanza alla vigente normativa sulla tutela dei dati personali (Codice Privacy), le cui procedure assicurano elevati livelli di sicurezza e controllo delle attività di utilizzo dei sistemi informatici da parte

degli addetti ad ogni livello.

Resta fermo che nello svolgimento delle attività tutti i destinatari del Modello sono tenuti ad osservare i principi generali di comportamento che la Società ha individuato in conformità anche a quanto previsto dal Codice Etico e dalle procedure in materia di protezione dei dati culminate nella redazione del DPS.

Si ribadisce inoltre che ogni operazione individuata ai fini del Modello come "sensibile" debba essere adeguatamente registrata e documentata ai fini della sua **"tracciabilità".** Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post* anche tramite appositi supporti documentali.

A tutte le risorse è tassativamente vietato:

- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico;
- intervenire illegalmente con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinente a danno dello Stato o di un Ente Pubblico per procurare direttamente o indirettamente un vantaggio o un'utilità all'ente;Conseguentemente è fatto espresso obbligo ai dipendenti, agli Amministratori, al Direttore Generale, ai Direttori di Farmacia ed ai Consulenti della Società di conoscere e rispettare:
- le disposizioni previste dal Disciplinare per la protezione dei dati con particolare riferimento alle misure di sicurezza poste in essere e da adottare;
- tutte le misure, anche non presenti nel Disciplinare per la protezione dei dati, atte a garantire l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o di perdita ed il rischio di accesso non autorizzato o non consentito.

Nell'ambito dei suddetti comportamenti, è tassativamente imposto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alle comunicazioni sociali;
- assicurare un pieno rispetto delle norme di legge e regolamenti, nonché delle procedure aziendali interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni anche per finalità di legge;
- predisporre efficaci piani di sicurezza e sistematici monitoraggi della rete interna (intranet) aziendale, al fine di evitare la commissione di reati.

Per "sistema informatico" s'intende un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile alle persone, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche".

5. Responsabilità

Nell'ambito delle attività in questione le responsabilità sono ripartite come segue:

- **Il Responsabile dei Sistemi Informativi** è responsabile dell'applicazione, aggiornamento e modifica del presente protocollo;
- il Responsabile di ciascuna area aziendale, nei limiti delle proprie competenze, adotta misure idonee ad evitare situazioni atte a facilitare la potenziale commissione dei reati menzionati

per la non osservanza delle disposizioni inerenti la sfera delle attività incluse nelle competenze dell'area Sistemi Informativi. Deve altresì segnalare tempestivamente all'Organismo di Vigilanza ogni evento suscettibile di incidere sull'operatività e sull'efficacia del protocollo stesso.

Qualora si verifichino circostanze:

- non espressamente regolamentate dal protocollo;
- che si prestano a dubbie interpretazioni/applicazioni;
- tali da originare obiettivi e gravi difficoltà di applicazione del protocollo medesimo;

è fatto obbligo a ciascun soggetto coinvolto nell'applicazione del presente protocollo di rappresentare tempestivamente il verificarsi anche di una sola delle suddette circostanze al proprio Responsabile che le riferirà con solerzia all'Organismo di Vigilanza; quest'ultimo valuterà gli idonei accertamenti in relazione alla singola fattispecie.

Ciascuna funzione aziendale è responsabile della veridicità, autenticità ed originalità della documentazione e delle informazioni rese nello svolgimento dell'attività di propria competenza.

6. Sistema disciplinare

Il presente protocollo costituisce una parte integrante del Modello organizzativo della Società. L'inosservanza dei principi e delle regole ivi contenuti rappresenta pertanto una violazione di detto Modello e comporta l'applicazione del Sistema disciplinare.