Título: **Norma Institucional Relacionada al Uso Apropiado de Estaciones de Trabajo**	REFERENCIA
Centro de Diabetes para Puerto Rico Administración y Recursos Humanos	Página 1 de 5
Aprobado por: Jorge De Jesús Rozas, MHSA	Efectivo: 23 de agosto de 2010 Revisado:

NORMA:

En el Centro de Diabetes para Puerto Rico las computadoras provistas son para el uso exclusivo de las operaciones del Centro y no pueden ser utilizadas para propósitos ajenos a la misión de esta corporación.

PROPOSITO:

1. Establecer las reglas de uso correcto de los recursos de computadoras en el Centro.

PERSONA(S) RESPONSABLE(S):

- *TODOS* los miembros de la fuerza laboral (empleados, facultad, enfermeras, estudiantes, voluntarios, etc.) del Centro de Diabetes así como contratistas y asociados cuando se encuentran realizando labores en las facilidades de la organización.

- *TODO* usuario de computadora y sistema de comunicación dentro de las facilidades del Centro, a todas las plataformas (sistemas operativos) y a todos los programas en usa, en combinación con la "*Política de Control de Acceso a Sistemas*".

CONCEPTOS GENERALES:

1. El uso de las computadoras del Centro deberá ser apropiado, legal y ético.

2. El Centro, mediante su Oficial de Seguridad de HIPAA, asegurará que los usos específicos de las computadoras sean cónsonos con esta política.

3. El Administrador del sistema asignará los accesos y cuentas de acuerdo a las funciones del usuario.

4. Todos los datos creados y guardados en las computadoras son propiedad del Centro.

VIGILANCIA:

1. La Administración tiene la responsabilidad de vigilar las actividades relacionadas con las computadoras para asegurar el uso correcto de las mismas para cumplimiento con esta y otras políticas.

2. La información recopilada obtenida por el uso incorrecto podrá ser utilizada como evidencia en acciones disciplinarias correctivas ó en acciones legales, si fuese necesario.

USO APROPIADO:

1. No se permitirán anuncios, ni campañas políticas ó religiosas en las computadoras del Centro.

2. Se prohibe el uso de computadoras del Centro para acceder ó propagar material obsceno, pornográfico, profano ó de algún modo objetable.

ACLARACION - Aunque esta política prohíbe el acceso a material inapropiado, los usuarios podrían acceder material ofensivo a través del Internet inadvertidamente. Mediante este aviso los usuarios son notificados sobre su responsabilidad por los sitios que ellos acceden y las repercusiones que esto pueda tener.

USO LEGAL:

1. No se permitirá ningún equipo que no tenga número de propiedad del Centro, conectados a la red de información, a menos que sea autorizado por el Coordinador de Sistemas de Informática ó por la necesidad de actualización ó diagnóstico de otros equipos.

2. Las computadoras no serán utilizadas para ninguna actividad ilegal.

3. Los miembros de la fuerza laboral se regirán por las leyes federales y estatales que regulan el uso de las comunicaciones y las computadoras.

4. El Centro considerará las siguientes actividades como "uso ilegal":

   a. Acoso de otros usuarios
   b. Difamación de algún usuario
   c. Destrucción ó daño de los equipos, programas ó información bajo custodia del Centro ó a algún otro usuario
   d. Interrupción ó monitoreo sin autorización de las comunicaciones electrónicas
   e. Copiar material con derechos reservados sin autorización
   f. Guardar en las computadoras del Centro información ilegal ó ilegalmente adquirida
   g. Violaciones a la confidencialidad y privacidad
   h. Violaciones a las licencias de programas
   i. *Utilización del correo electrónico para usos no aprobados por la administración del CDPR*

USO ETICO Y ACEPTABLE

1. Las computadoras deberán ser utilizadas de acuerdo con los estándares de ética y misión del Centro. Cualquier uso que no cumpla con estas premisas podrá considerarse "usos inaceptables de los recursos del Centro".

2. Algunos usos inaceptables pudieran repercutir en consecuencias legales si se viola alguna ley y derechos de alguna entidad ó persona; en cuyo caso el usuario pudiera ser responsable y tener que indemnizar por sus acciones ó usos al Centro.

3. El Centro considerara las siguientes actividades como "usos inaceptables":

    a. Violación del sistema de seguridad de las computadoras
    b. Violación a las guías, a las políticas y regulaciones de utilización de la red de computadoras.
    c. Utilización de cuentas de computadoras, códigos de accesos ó números de identificación en la red pertenecientes a otro usuario.
    d. Utilización de computadoras de manera que innecesariamente impida el funcionamiento ó labor de otros.
    e. Acceso inapropiado para acceder y compartir información de salud protegida del paciente.
    f. Acceso al Internet para uso no cónsono con la misión del Centro.

4. El Centro y su fuerza laboral reconocen que los equipos de computadoras conectados a las redes del Centro, son recursos que facilitan las tareas que se llevan a cabo.

5. El Centro solicitará que los miembros de su fuerza laboral ejerzan las siguientes consideraciones en apoyo del espíritu "cooperativo" de sus recursos:

    a. Uso prudente del servicio de correo electrónico y resguardo prudente de las comunicaciones.

    b. Consideración en el tiempo que se utilizan las computadoras

USO DEL CORREO ELECTRONICO ("EMAIL"):

1. El Centro y su fuerza laboral reconocen que el uso de correo electrónico no es un medio seguro de comunicación.

2. El Centro advertirá sobre la necesidad de tener precaución al dirigir correos a direcciones electrónicas agrupadas.

3. El correo electrónico interno ("Intranet") podrá tener información protegida acerca de la salud de los pacientes (PHI).

4. Correo interno con PHI debe adherirse a lo siguiente:

    a. El que recibe el comunicado debe tener una necesidad válida para tener acceso a la información.
    b. La transmisión de PHI debe ser para propósitos de tratamiento, pago u operaciones.
    c. La distribución de transmisiones se deben limitar al mínimo de recipientes posible.
    d. Se utilizarán de medidas adicionales de seguridad tan pronto se hagan disponibles.

El envío de correo electrónico con PHI hacia el exterior ("Extranet) está prohibido.

CONTRASEÑAS Y ACCESOS AL SISTEMA:

1. Los usuarios NO deberán hacer públicas sus cuentas ni contraseñas; NUNCA BAJO NINGUNA CIRCUNSTANCIA NI RAZON, .DEBERAN SER DIVULGADOS A OTROS.

2. Los supervisores ó gerentes no requerirán a sus subalternos que le divulguen sus contraseñas o alguna otra información sobre sus cuentas de acceso particulares a menos que estén autorizados para ello por el Oficial de Seguridad, el Oficial de Cumplimiento ó la Administración.

3. Las contraseñas, códigos de acceso, códigos secretos, "tokens", nombres de usuarios, así como los mecanismos utilizados para acceder los sistemas del Centro se tratarán como información confidencial.

4. Las contraseñas no deben ser fáciles de adivinar y deberán ser mayores de ocho (8) caracteres (letra, número y/ó símbolos).

5. Las contraseñas no deberán ser igual al nombre de cuenta o usuario.

6. Los usuarios ***no*** podrán tener más de una cuenta de acceso.

7. Los usuarios son responsables por todo el trabajo realizado bajo su cuenta de acceso por lo que:

    a. Serán responsables de terminar sus sesiones de comunicación (desconectarse) apropiadamente.

    b. Asegurarse que nadie tenga acceso a su cuenta.

8. Los controles de acceso a programas deben ser únicos para confiar en las auditoras de utilización y acceso de los sistemas.

9. Si un usuario tiene razones para pensar que alguien ha utilizado o aprendido su identificación, contraseña ó cuenta de acceso, deberá notificarlo inmediatamente a su supervisor, director de sistemas al Oficial de Seguridad; y el asunto se debe atender de inmediato. Para proteger aún más su contraseña, el usuario no deberá escribir la misma en un sitio accesible a otros usuarios.

10. Los supervisores, gerentes o sus designados son responsables de notificar cambios requeridos en cuentas de usuarios debido a cambios de nombre, clasificación, requerimientos de trabajo, etc.

11. Cualquier terminación de cuentas debe ser reportada de inmediato para tomar medidas inmediatas.

VISIBILIDAD DE ESTACIONES / TERMINALES DE TRABAJO:

1. Las estaciones ó terminales de trabajo estarán localizadas de manera tal que la información desplegada en sus pantallas esté protegida de divulgación inadvertida por personas que pasen cerca de estas y que puedan ver su información.

2. Protectores de pantallas ("screen savers") pudieran ser utilizados para proveer seguridad visual adicional.

Programas (Software)

1. Solamente programas con licencia y aprobados, revisados e instalados por el personal de Sistemas de Informática pueden ser utilizados en las computadoras provistas por el Centro.

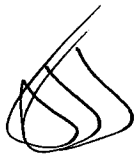
2. Los usuarios no harán copias ilegales de programas de ningún tipo.

En adición a medidas disciplinarias del Centro, el usuario será responsabilizado por gastos en los que se incurra como resultado de cualquier acción por tal uso ilegal.

SANCIONES, ACCIONES CORRECTIVAS Y DISCIPLINARIAS:

Violaciones a lo establecido en esta Política conllevará sanciones y/o acciones correctivas ó disciplinarias.

Aprobado por:



Jorge De Jesús Rozas, MHSA
Director Ejecutivo