I. POLÍTICA

Esta política establece un marco dentro de cual el centro resuelva requisitos para alcanzar secreto y seguridad de toda la información protegida. Todas las personas implicadas con la creación, la colección, la dirección y/o la difusión de la información médica confidencial están conforme a las condiciones de esta política. Esto incluye a todos los miembros del personal, los voluntarios, los aprendices, los estudiantes y cualquier otro individuo que tengan acceso a la información confidencial.
La información confidencial incluye la información protegida paciente de la salud, información del empleado, información financiera, información del negocio comunicada y/o almacenada de cualquier manera, incluyendo verbalmente, vía fax u otros medios de la telecomunicación, en el papel, o en cualquier otra forma electrónica.

II DEFINICIONES DE LA INFORMACIÓN CONFIDENCIAL

A. Información Protegida de la Salud

El acto de la portabilidad y de la responsabilidad del seguro médico (HIPAA), 45 partes 160 y 164 de CFR, define la información protegida de la salud (PHI) como:

1. Información individualmente identificable de la salud, incluyendo la información demográfica;
2. Recogido de un individuo o creado sobre un individuo por un abastecedor del cuidado médico, plan de la salud, historia de empleo;
3. Se relaciona con la salud última, actual o futura o la condición física o mental de un individuo; o el pago último, actual o futuro para la disposición del cuidado médico a un individuo;
4. Eso identifica el individuo, o con respecto cuál hay una base razonable a creer a la información puede identificar al individuo.
5. La información protegida de la salud se puede mantener adentro o transmitir con cualquier medio, incluyendo forma (electrónica) verbal, escrita, registrada (cinta o digital), o automatizada.
6. El sistema de registro señalado es un subconjunto de la información protegida de la salud que reside en los expedientes médicos y es mantenido por el centro de Schreiber Pediatric Rehab y utilizado por el centro tomar decisiones sobre clientes. Vea la gerencia de expedientes de # 504 de la política y el control médicos, política en la derecha de solicitar el acceso y la enmienda al sistema de registro señalado.

B. Información del empleado

La información del empleado se mantiene en escrito, registrado (cinta o digital), película, forma (electrónica) automatizada, verbalmente en cualesquiera más allá de, actual o futuro empleado del centro. Las fuentes primarias de esta información son personales (los curriculums vitae, las evaluaciones de funcionamiento), el sistema de la nómina de pago (es decir. sueldos del empleado) y servicio médico de empleado (expedientes de la salud de empleado). Esta información se considera confidencial. Las preguntas con respecto a lanzamiento de esta información refirieron al coordinador de los recursos humanos. El empleo del médico y la información credentialing son mantenidos en archivos de la oficina del presidente.

Información del negocio

C. La información del negocio

La información del negocio se mantiene en escrito, registrado (cinta o digital), película, forma (electrónica) automatizada, o verbalmente con respecto al estado del centro. Los ejemplos de la información del negocio incluyen:

1. Financiero (rédito, presupuestos)
2. Comercialización (resultados de la encuesta sobre satisfacción de cliente)
3. Personal clínico (Credentialing, revisión de par)
4. Planeando (plan de la construcción, planes estratégicos)
5. Operacional (Scheduling)
6. Seguridad (datos de la gerencia de riesgo)
7. Educación (expedientes del entrenamiento)

III RESPONSABILIDADES DE ORGANIZACIÓN

A. Aplicaciones y accesos

1. No utilizaremos ni divulgaremos la información protegida de la salud excepto según lo permitida o requerida por ley federal y del estado. El acceso de la información protegida de la salud será realizado por el personal entrenado de acuerdo con nuestro secreto de la política #502 de expedientes y estado médico y los leyes federales.
2. No intimidaremos, no amenazaremos, no forzaremos, no discriminaremos contra, ni tomaremos cualquier otra acción vengativa contra cualquier individuo que ejercite la cualquier derecha protegida de la aislamiento de la información de la salud debajo de HIPAA, incluyendo la limadura de una queja con el funcionario de la aislamiento del centro o la secretaria de los servicios de salud y humanos y de la declaración, de asistir, o de participar en los procedimientos u oír de una investigación asociados a tal queja.
3. Que la voluntad supervisa rutinariamente a trabajadores' tienen acceso a y acceso de la información protegida de la salud y de otros expedientes confidenciales para asegurar conformidad con la política, e iniciaremos la acción correctiva para prevenir cualquier abertura del secreto, de la violación de las derechas de la aislamiento o de los incidentes de la seguridad que dé lugar a la abertura del secreto, a la alteración de la integridad de datos, o a la interrupción de la información protegida de la salud o de cualquier otra información confidencial.
4. Atenuaremos, al grado practicable, a cualquier efecto dañoso de un uso o al acceso de la violación protegida de la información de la salud de políticas y de procedimientos que se sabe para haber sido realizada por nosotros o por uno de nuestros socios.

B. Políticas, procedimientos y documentación

1. Tendremos políticas y los procedimientos que protejan el secreto y la seguridad de los derechos protegidas de la información de la salud información de la salud de nuestros clientes', y el secreto y la seguridad de la otra información confidencial.
2. Siempre que haya un cambio en la ley que afecta materialmente el contenido del aviso de las prácticas de la privacidad, haremos revisiones apropiadas y diseminaremos la nueva versión. La política y el aviso revisados de las prácticas de la aislamiento serán publicados la misma fecha.
3. Mantendremos políticas y procedimientos revisados en forma escrita o electrónica en perpetuidad. Políticas, se han cambiado, serán retiradas pero no suprimidas que de nuestra documentación de la política y de procedimiento.

4. Mantendremos la otra documentación necesaria para conformarse con las regulaciones de la aislamiento y de la seguridad de HIPAA por siete años, incluyendo pero no limitadas:
    - ❑ Reconocimiento del recibo del aviso de las prácticas de la aislamiento
    - ❑ Las acciones se asociaron a las quejas, incidentes, mitigación, y aplicaron sanciones
    - ❑ Autorizaciones para las aplicaciones y los accesos de la información protegida de la salud
    - ❑ Contratos del socio - designaciones de entidades cubiertas afiliadas y de arreglos organizados del cuidado médico
    - ❑ Los documentos se asociaron al proceso debido de las derechas pacientes
    - ❑ Evidencia de la educación, del entrenamiento y del conocimiento

C. Notificación del Confidencialidad y de la Seguridad/Declaración del Reconocimiento
1. Cada miembro de nuestra mano de obra firmará el Confidencialidad y la Seguridad de la Notificación de la información/de la declaración del reconocimiento. (Véase el accesorio A)
2. El coordinador del recurso humano manejará la confidencialidad y la Seguridad de la Notificación de la información/de la declaración del reconocimiento para el coordinador del empleado y voluntario para los voluntarios.

D. Educación del Confidencialidad y de la Seguridad, Entrenamiento y Conocimiento
1. El centro establecerá programas de la educación, del entrenamiento y del conocimiento para comunicar las políticas como apropiadas.
2. Categorizarán a los miembros de la mano de obra según el nivel del acceso a la información confidencial. La educación trataría los niveles del acceso a la información confidencial.
3. Todos los miembros de la mano de obra recibirán recordatorios educativos obligatorios anuales en las políticas y los procedimientos del secreto, privacidad y seguridad de la información protegida de la salud. El tipo, la cantidad, la fecha y los nombres del personal que reciben esta educación se mantienen la oficina del coordinador de los recursos humanos.
4. En una base en curso, proporcionaremos recordatorios sobre y el conocimiento para el secreto, la aislamiento y la seguridad de la información de la salud con una variedad de modalidades.
5. A empezar el nuevo trabajo, cada miembro de la mano de obra recibirá una orientación al confidencialidad, a la privacidad, y a los conceptos de la seguridad del confidencialidad según lo contorneado en esta política.
6. Entrenarán a los usuarios de nuestros sistemas de información también en cómo utilizar las aplicaciones informáticas específicas necesitadas para hacer el trabajo para la posición a la cual los están empleando, se están transfiriendo, o se están contratando de otra manera, incluyendo pero no limitadas:
    - ❑ Confidencialidad del código de acceso y selección de la contraseña, mantenimiento y uso.
    - ❑ Supervisión de la capacidad a la conexión y divulgación de las faltas de la conexión.
    - ❑ Esfuerzos de mantener la seguridad del ambiente de computadora (es decir, cortafuegos, protección del virus; transacciones desautorizadas de la información protegida de la salud).

- Uso apropiado del E-mail y del Internet, si se concede tal acceso.
- Prohibición en el uso de los programas desautorizados del software de incluir ahorradores de la pantalla, juegos y otros tales programas a menos que esté autorizado para uso del funcionario de la seguridad de la información del centro.
- Otros componentes dominantes de las políticas se relacionaron con el secreto y la seguridad. Funcionario de la privacidad de la información y funcionario de la seguridad de la información

E. Funcionario de la privacidad de la información y funcionario de la seguridad de la información

Emplearemos a individuo para servir como el funcionario de la privacidad para la organización. Seleccionarán al funcionario de la privacidad proporcionar el secreto para la información protegida de la salud. El funcionario de la privacidad es responsable de desarrollar un programa para asegurar el secreto y la privacidad de toda la información protegida de la salud. El funcionario de la privacidad proporciona descuido en el desarrollo de la política y del procedimiento que afecta la información protegida de la salud. El número de teléfono del funcionario de la privacidad será fijado a través de la organización en caso que un cliente, un padre o un miembro de la mano de obra del centro elija para archivar una queja

Esta misma información debe ser proporcionada toda la correspondencia de organización referente a la información protegida de la salud. El funcionario de la aislamiento es responsable de documentar y de investigar cualquier queja del cliente o del miembro de la mano de obra con respecto a la información protegida de la salud.

1. El centro empleará a individuo para servir como el funcionario de la seguridad de la información para la organización. El funcionario de la seguridad de la información coordinará todos los aspectos de la seguridad referente a la información protegida de la salud con el funcionario de la aislamiento de la información que es responsable de determinar riesgos de la seguridad y de desarrollar un programa para atenuar riesgo. El funcionario de la seguridad de la información es responsable de convertirse y las políticas el poner en ejecución y los procedimientos administrativos , físicos y técnicos. El funcionario de la seguridad de la información es responsable de documentar y de investigar incidentes de la seguridad de la información.

IV RESPONSABILIDAD de la GERENCIA (aplicable a todos los empleados o contratistas que supervisan a miembros de nuestra mano de obra)

A. Se esperará que los jefes de servicio documenten los procedimientos del secreto y de la seguridad específicos a sus requisitos del personal. Estos procedimientos deben ser constantes con políticas organización-anchas.
B. El entrenamiento específico del secreto, de la aislamiento y de la seguridad debe ser proporcionado por cada departamento por funciones de trabajo y requiere el entrenamiento.
C. Los jefes de servicio deben tomar la acción apropiada para las violaciones de la privacidad o la abertura sospechadas o divulgadas de la seguridad acción disciplinaria como apropiada. Los recursos humanos se deben entrar en contacto con referente a las sanciones aplicadas a los empleados.

V RESPONSABILIDAD DE LOS MIEMBROS DE LA MANO DE OBRA

A. Repase y conviértase al corriente de las políticas y de los procedimientos relacionados con la seguridad del secreto y de la información.
B. Firme el secreto y la seguridad requeridos de la notificación de la información/de la declaración y del acuerdo del reconocimiento a estas políticas.
C. Tenga acceso solamente a la información requerida para realizar deberes del trabajo.
D. Divulgue cualesquiera violaciones de la privacidad o incidente sospechadas de la seguridad al supervisor inmediato.
E. Mantenga las contraseñas de una manera segura. Divulgue las contraseñas o el user-id perdidas o robadas inmediatamente al funcionario de la seguridad de la información.
F. Vuelva a la pantalla sign-on al salir de un sitio de trabajo.
G. Disponga no más impresa o escrita de la información confidencial funcionando de una manera segura por ejemplo destrozando.
H. Entre en contacto con a funcionario de la aislamiento del centro si hay preguntas con respecto secreto, aislamiento o a la seguridad de la información.

VI POLÍTICA PREPARADA Y APROBADA: 14 de marzo de 2003

VII FECHA REVIEWED/REVISED: Julio de 2008, el julio de 2011, 9/2012

_____

Presidente