



MANUAL PARA EL MANEJO DE LA INFORMACION EN EL RW CAREWARE

El propósito principal del Manual para Manejo de la Información en el Sistema RW CAREWare es ofrecer a todo el personal, que de alguna manera u otra tiene acceso a la información de las PVVS (Personas viviendo con VIH o SIDA), ya sea sociodemográfica, clínica o de apoyo, una herramienta de seguridad para proteger la privacidad y confidencialidad de la información de las PVVS.

NOVIEMBRE 2018

OBJETIVOS

MANUAL PARA MANEJO DE LA INFORMACIÓN EN EL SISTEMA RW CAREWARE

El propósito principal del *Manual para Manejo de la Información en el Sistema RW CAREWare* es ofrecer a todo el personal, que de alguna manera u otra tiene acceso a la información de las PVVS (*Personas viviendo con VIH o SIDA*), ya sea sociodemográfica, clínica o de apoyo, una herramienta de seguridad para proteger la privacidad y confidencialidad de la información de las PVVS.

El Programa *Ryan White* Parte A recibe diariamente información por métodos electrónicos a través del *RW CAREWare*.

Los objetivos del manual son los siguientes:

1. Establecer las guías para mantener un sistema uniforme y eficiente en la protección de la confidencialidad, privacidad y seguridad de la información de las PVVS, tanto sociodemográfica como clínica.
2. Establecer las guías para el mejor manejo de la información de las PVVS, de tal forma que haya uniformidad y eficiencia en los servicios a prestarse.
3. Servir de guía al personal que labora en el Programa *Ryan White* Parte A sobre las funciones, normas y los procedimientos a seguir en la protección de la confidencialidad y privacidad de la información de las PVVS.
4. Servir de guía para la orientación y adiestramiento de empleados nuevos y re-adiestramiento de todo el personal del Programa *Ryan White*.
5. Servir de guía y referencia a evaluadores de las agencias acreditadoras y certificadoras del Programa *Ryan White* Parte A.
7. Facilitar la dirección, supervisión, coordinación y labor de todo el personal del Programa *Ryan White* Parte A, que utilizan de una forma u otra la información de las PVVS.

Es importante custodiar y mantener seguros los expedientes clínicos, para garantizar el mantenimiento de la documentación requerida por las agencias federales y estatales de forma eficiente, accesible y segura. El *RW CAREWare* es el único instrumento de medida cualitativa y cuantitativa del servicio clínico que utiliza el programa *Ryan White* Parte A, además de que la información contenida en *RW CAREWare* representa la evidencia legal y financiera; y sirve como herramienta de comunicación entre el personal autorizado a trabajar con las necesidades clínicas y de apoyo a nuestros pacientes.

NORMAS GENERALES

1. Todo el personal será orientado sobre las leyes de Privacidad y Confidencialidad que protegen la información de salud protegida del paciente. Se tomará la firma a todo el personal conforme sea orientado en el Acuerdo de Confidencialidad y No-Divulgación. Este documento se ubicará en el expediente del empleado del Programa *Ryan White*.
2. Todo el personal de aquellas agencias o programas con las que el AME de San Juan mantiene una relación de trabajo que implique el manejo de información de salud de pacientes, será orientado sobre las leyes de Privacidad y Confidencialidad que protegen la información de salud protegida del paciente. Se le tomará la firma a todo el personal, conforme sea orientado en el Acuerdo de Confidencialidad y No – Divulgación.
3. Todo el personal será orientado sobre las siguientes políticas:
 - a. Cumplimiento con la seguridad electrónica del AME de San Juan
 - b. Política de uso apropiado de estaciones de trabajo
 - c. Consideraciones relacionadas a la Confidencialidad y Privacidad de la información en el uso de computadoras

I. INTRODUCCION AL CUMPLIMIENTO CON LA SEGURIDAD ELECTRÓNICA DEL AME DE SAN JUAN

El AME de San Juan es una entidad cubierta bajo las disposiciones de la *Health Insurance Portability and Accountability Act* del 1996 (conocida como Ley *HIPAA*), Ley Pública Número #104-191 del 21 de agosto de 1996.

Las Reglas de Seguridad Electrónica de la Ley *HIPAA* exigen que toda entidad cubierta y sus Asociados de Negocios que crean, reciben, mantienen y/o transmiten electrónicamente información de salud, guarden la confidencialidad, privacidad, integridad y seguridad de la misma. Las reglas sobre esta información de salud se conocen como *electronic Protected Health Information* y se identifica por sus siglas en inglés como *e-PHI*.

El AME de San Juan creará y establecerá políticas y procedimientos para mantener, asegurar y/o resguardar la información de salud protegida, que se almacenará en forma electrónica (*e-PHI*, por sus siglas en inglés) para prevenir que las situaciones fuera de control como por ejemplo: fuego; terremoto; vandalismo; fallas en los sistemas; desastres naturales; entre otros, que imposibiliten la misión de la organización o el acceso a el *e-PHI*, alteren el *e-PHI* y/o no se pueda acceder el *e-PHI* en su estado original.

Esta regulación aplica a todos los sistemas computadorizados que almacenen, manejen o transmitan el *e-PHI* y que sean críticos para continuar la operación o misión de la organización y a todos los empleados que sean designados para trabajar en situaciones de emergencia o contingencia o que sean usuarios de los sistemas computadorizados.

La entidad cubierta deberá:

1. Asegurar la integridad y disponibilidad del *e-PHI* (45 CFR-164-306 (a))
2. Proteger la *e-PHI* frente a peligros o amenazas que razonablemente puedan ser previstos
3. Proteger la seguridad o integridad de la información
4. Proteger contra usos y divulgaciones no autorizadas por las reglas
5. Crear y poner en práctica normas y procedimientos para garantizar el cumplimiento por la fuerza laboral (45CFR 164-306(a))

Como parte del cumplimiento, es necesario que todo empleado del AME de San Juan y de las Organizaciones Sub Recipientes, salvaguarde y proteja la integridad, confidencialidad y seguridad de la *e-PHI* conociendo las disposiciones legales y reglamentarias que así lo exigen.

Una Brecha de Confidencialidad es la pérdida de información de salud protegida, de uno o más pacientes, por medios electrónicos. Si esta situación ocurriese, la misma deberá reportarse inmediatamente a la Directora del AME de San Juan. Esta a su vez lo notificará a la Oficina de Asuntos Legales y Ley *HIPAA* del Municipio de San Juan, para una consulta con un Asesor Legal y realizar la investigación pertinente.

Por consiguiente, es deber de todo empleado del AME de San Juan y de las Organizaciones Sub Recipientes el manejar el *e-PHI* y el equipo electrónico que le sea asignado conforme con los procesos y procedimientos, órdenes administrativas y reglamento creados por el AME de San Juan.

El incumplimiento con lo anterior podría resultar en la imposición de medidas disciplinarias y/o sanciones legales.

II. POLITICA DE USO APROPIADO DE ESTACIONES DE TRABAJO (COMPUTADORAS)

Propósito

Esta política tiene como propósito establecer las normas de uso para los recursos de computadoras.

Alcance

Esta política aplica a todos los miembros de la fuerza laboral del AME de San Juan, así como contratistas y Organizaciones Sub Recipientes que se encuentran realizando labores dentro y fuera de las facilidades de la Organización.

Conceptos Generales de la Política de Monitoreo de los Sistemas Computadorizados

- El uso de computadoras del AME de San Juan deberá ser apropiado, legal, ético y cooperativo.
 - I. El AME de San Juan y el personal de administración del *RW CAREWare* tomarán decisiones, según sean necesarias, para que los usos específicos de las computadoras sean cónsonos con esta política.
 - II. El personal de administración del *RW CAREWare* será la autoridad final en el uso de las computadoras, así como en el otorgamiento de acceso y cuentas.
 - III. Todos los datos creados y/o guardados en las computadoras del AME de San Juan, se convertirán en propiedad del AME de San Juan.

A. Monitoreo de los Sistemas Computadorizados

- El Personal designado en el AME de San Juan tiene derecho de monitorear las actividades de las computadoras, para asegurar el uso correcto de las mismas para el cumplimiento con esta y otras políticas.
- La información recopilada durante el monitoreo será discutido en el comité asesor de RW CAREWARE y podrá ser utilizado como evidencia en acciones disciplinarias o correctivas, o en acciones legales, de ser necesario.

B. Uso apropiado

- Los equipos de computadoras provistos por el AME de San Juan son para uso exclusivo de las operaciones de negocio del AME de San Juan y no pueden ser utilizados para propósitos ajenos a la misión de la organización.
- No se permitirán anuncios ni campañas políticas o religiosas en las computadoras del AME de San Juan, ni acceder a propaganda o material obsceno, pornográfico, profano o de algún otro modo objetable.
- Cualquier equipo computadorizado ajeno (que no sea propiedad o provisto por el AME de San Juan) y que sea utilizado para el sistema RW CAREWare (o que lo tenga instalado) le aplican todas las políticas y procedimientos establecidos por este manual.

C. Uso Legal

1. Las computadoras no serán utilizadas para ninguna actividad ilegal.
2. Los empleados del AME de San Juan y Organizaciones Sub Recipientes, se regirán por las leyes estatales y federales que regulan el uso de las comunicaciones y las computadoras.
3. El AME de San Juan considerará las siguientes actividades, como actividades de uso "ilegal" :
 - Acoso a otros usuarios
 - Difamación a algún usuario
 - Destrucción o daños a los equipos, programados o información bajo la custodia del AME de San Juan o algún otro usuario
 - Interrupción o monitoreo sin autorización de las comunicaciones electrónicas
 - Copiar material con derechos reservados sin autorización
 - Guardar en las computadoras del AME de San Juan, información ilegal o ilegalmente adquirida
 - Violaciones a la CONFIDENCIALIDAD
 - Violaciones a las licencias de programados

D. Uso ético y aceptable

Las computadoras deben ser utilizadas de acuerdo con los estándares de ética y misión del AME de San Juan. Cualquier uso que no cumpla con esta premisa debe considerarse “uso inaceptable”:

- Violación del sistema de seguridad de las computadoras
- Utilización de cuentas de computadoras, código de accesos o números de identificación en la red pertenecientes a otro usuario
- Utilización de computadoras, de manera que innecesariamente impida el funcionamiento o labor de otros
- Acceso inapropiado para acceder y/o compartir información socio-demográfica y de salud del paciente
- Violaciones a las políticas y regulaciones de utilización de la red
- Violación a la privacidad de otro usuario

E. Uso Cooperativo

El AME de San Juan y su fuerza laboral reconocen que los equipos de computadora conectados a las redes del Programa *Ryan White*, Incluyendo las Organizaciones Sub Recipientes, son recursos que facilitan las tareas que se llevan a cabo, por lo que la utilización es “cooperativa”.

El AME de San Juan solicitará que sus empleados ejerzan las siguientes consideraciones, en apoyo del espíritu cooperativo de sus recursos:

1. Uso prudente del servicio de correo electrónico y resguardo prudente de las comunicaciones
2. Consideración en el tiempo que se utilizan las computadoras
3. Consideración en el espacio utilizado para guardar la información
4. Consideración en los recursos de impresión
5. Consideración en la capacidad de datos de la computadora
6. Consideración a los derechos y privilegios de los demás usuarios

En situaciones donde varios empleados se encuentren aglomerados alrededor de una pantalla de alguna estación, el empleado de esa estación deberá cerciorarse de que aquellos que se encuentran allí tengan derecho o acceso a ver dicha información, para que se pueda dar el uso “cooperativo”.

F. Uso del Correo Electrónico (Email)

El AME de San Juan y sus empleados reconoce que el uso del correo electrónico no es un medio seguro de comunicación.

El AME de San Juan advertirá sobre la necesidad de tener precaución al dirigir correos a direcciones electrónicas agrupadas.

El correo electrónico interno (*Intranet*) podrá tener información protegida de salud (*PHI*, por sus siglas en inglés)

Correo interno con *PHI* debe adherirse a lo siguiente:

1. El que recibe el comunicado debe tener una necesidad válida para tener acceso a la información
2. La transmisión de *PHI* debe ser para propósitos de tratamiento, pago u operaciones
3. La distribución de transmisiones se debe limitar al mínimo de recipientes posibles
4. Se recomienda el uso de medidas adicionales de seguridad para proteger el contenido de la información, como: uso de criptografía; cifrado, firmas electrónicas y aviso de confidencialidad, tan pronto se hagan disponibles.

El envío de correo electrónico con *PHI* hacia el exterior (*Extranet*) está prohibido, a no ser que se utilicen medidas de criptografía para proteger su contenido.

G. Contraseñas (Passwords) y accesos al sistema RW CAREWare

Los usuarios no deberán hacer pública sus cuentas ni contraseñas: NUNCA, BAJO NINGUNA CIRCUNSTANCIA NI RAZON, DEBERAN SER DIVULGADAS A OTROS.

Se cambiarán los *PASSWORDS* regularmente y se revisarán los niveles de acceso de las personas.

Los Supervisores o Gerentes no requerirán a sus subalternos que se divulguen sus contraseñas o alguna información sobre sus cuentas de acceso a particulares, a menos que estén autorizados para ello por la Administración.

Las contraseñas; códigos de acceso; códigos secretos; *tokens*; nombres de usuarios, así como los mecanismos utilizados para acceder los sistemas del AME de San Juan, se tratarán como información confidencial.

- Las contraseñas **no** deben ser fáciles de adivinar y deben ser mayores de 8 caracteres
- Las contraseñas no deberán ser igual al nombre de cuenta o usuario
- Los usuarios podrán tener más de una cuenta de acceso, dependiendo de sus funciones
- Los usuarios son responsables por todo el trabajo realizado bajo su cuenta de acceso, por lo que:
 - Serán responsables de terminar sus sesiones de comunicación (desconectarse) apropiadamente
 - Asegurarse de que nadie tenga acceso a su cuenta

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

Si un usuario tiene razones para pensar que alguien ha utilizado o aprendido su identificación, contraseña o cuenta de acceso, deberá notificarlo inmediatamente a su supervisor o gerente de sistemas y el asunto se debe atender de inmediato.

Los supervisores, gerentes o personal designado son responsables de notificar cambios requeridos en cuentas de usuarios debido a cambios de nombre, clasificación, o requerimientos de trabajo.

Los empleados firmarán el documento: *CONSENTIMIENTO DEL DEL USUARIO*.

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

H. Visibilidad de Estaciones

Las estaciones o terminales están localizadas de manera tal que la información desplegada en sus pantallas está protegida de divulgación inadvertida por personas que pasen por estas y que puedan ver su información

El AME de San Juan deberá velar porque los sistemas sean seguros. Para ello, se recomienda que los terminales o áreas donde estén localizadas las computadoras posean un mecanismo que los apague automáticamente cuando lleven un tiempo determinado sin usarse para evitar que alguien tenga acceso al sistema si el usuario se ha levantado sin apagar el sistema.

Protectores de pantallas (*screen saver*) deben ser utilizados para proveer seguridad adicional.

El Sistema *RW CAREWare* debe negar el acceso a la cuenta de los usuarios, cuando se cumpla un mínimo de 5 minutos sin actividad en el sistema.

I. Programas

Solamente los programas con licencia y aprobados, revisados e instalados por personal del AME de San Juan pueden ser utilizados en las computadoras provistas por el AME de San Juan.

Los usuarios NO harán copias ilegales de programas de ningún tipo.

En adición a medidas disciplinarias del AME de San Juan, el usuario será responsabilizado por gasto en los que se incurra como resultado de cualquier acción o

J. Uso del teléfono

Todo personal que ofrezca información confidencial por teléfono, deberá tomar todas las medidas para garantizar la confidencialidad de la información y deberá atender la

llamada desde su área de trabajo. Es de suma importancia que se confirme la identidad y la legitimidad de la persona a la que se le va a ofrecer la información.

De ninguna manera se permitirá divulgar información contenida en el CAREWARE usando un teléfono a ninguna persona.

K. Sanciones, acciones correctivas y medidas disciplinarias

Cualquier violación a lo establecido en esta política conllevará sanciones según especificado en el Manual de Medidas Disciplinarias del AME de San Juan.

III. POLITICA DE SEGURIDAD FISICA

Propósito

El AME de San Juan ha establecido políticas aceptables para establecer un nivel de seguridad física de los equipos electrónicos.

A tales efectos, se establecen requisitos de identificación y restricciones de acceso del personal.

Política

Todos los equipos electrónicos que incluyen sistema de cómputos, tienen que estar levantados del suelo para evitar que sufran daño en caso de inundaciones.

Áreas con información sensible están limitadas a personal autorizado o a personas con una razón importante de presencia.

Ninguna persona que no sea de la fuerza laboral del AME de San Juan podrá estar o utilizar área o sistemas con información sensible de la institución, a menos que haya sido previamente autorizado por un oficial de la organización.

Todo visitante, contratista o persona que no sea de la fuerza laboral del AME de San Juan, y que se encuentre en áreas con *PHI*, *e-PHI* o utilizando sistema con acceso a *PHI* o *e-PHI*, estará acompañado por personal del AME de San Juan en todo momento.

IV. CONSIDERACIONES SOBRE EL USO DE LAS COMPUTADORAS Y LA CONFIDENCIALIDAD

Algunas consideraciones son:

Las facilidades de cuidado de salud, al igual que todas las Organizaciones Sub Recipientes que reciben información del paciente, deben crear políticas que asegure la confidencialidad y privacidad de la información del paciente cuando sea electrónica o vaya a ser transmitida electrónicamente.

El Director o Gerencial asignado tiene a su haber el beneficiar al paciente, al proveedor y a la sociedad protegiendo el derecho individual de la privacidad.

La documentación de datos socio-demográficos, clínicos, o financieros que identifican al paciente, convierten el documento en uno confidencial y legal. La confidencialidad de la información clínica está fundamentada en los estatutos establecidos por el Estado y la Institución. Además está formulada en el código de ética de los profesionales de la salud, es por eso su impacto o implicaciones legales.

En la transmisión de información del paciente de forma electrónica, deben existir medidas de control que garantice la confidencialidad de la información en todo momento.

El avance en la tecnología, el aumento en la necesidad y el uso de la información de salud, hacen que esta pueda ser más accesible y vulnerable. Existe el acceso casual y el acceso malicioso.

Def. Acceso Casual al e-PHI: La violación a la confidencialidad por casualidad, es inaceptable. Individuos autorizados (o no autorizados) que tengan acceso a la información de salud por curiosidad y no como parte de su trabajo, son un ejemplo de acceso inapropiado de la información.

Def. Acceso Maliciosa al e-PHI: La violación a la confidencialidad maliciosa ocurre cuando un individuo autorizado (o no autorizado) tiene acceso a la información del paciente (salud, personal, financiera, etc.), con intención de causar daño intencionado y premeditado, siendo esto castigado por las leyes estatales y federales.

La gerencia del *RW CAREWare* es responsable de:

- I. Identificar estrategias y acercamientos efectivos que provean al Programa información acerca de las necesidades de mejoramiento y el uso de los servicios
- II. Revisar protocolos de trabajo y junto a las otras unidades del Programa, buscar el desarrollo de procedimientos que sirvan para mejorar los servicios directos a las personas con VIH
- III. Preparación de planes de trabajos e informes de progreso del Programa

Los proyectos que utilizan la información recopilada en el sistema *RW CAREWare* son los siguientes:

- Concejo de Planificación de *Ryan White* Parte A
- Programa de Calidad *Ryan White* Parte A
- Evaluación de procesos internos
- Seguimiento al cumplimiento con las medidas de ejecutoria establecidas por *HRSA (RW CAREWare)*
- Comité Inter-Partes *Ryan White*

Una de las herramientas que se utiliza para la gran mayoría de los proyectos arriba mencionados, informes, investigaciones y/o estudios, es el *RW CAREWare*. El *RW CAREWare* es un *software* gratuito, para la gestión y supervisión de la atención clínica y de apoyo del VIH, que produce informes estadísticos completos. Este programa fue lanzado por *HRSA (Health Resources and Services Administration)* en el año 2000. Su uso ha aumentado constantemente cada año, y hoy sobre 800 agencias que reciben fondos *Ryan White* en 48 estados, Puerto Rico y las Islas Vírgenes Americanas utilizan este *software* para administrar su información sobre el VIH/SIDA

Existen 2 formas de reportar los servicios ofrecidos a las PVVS a través del *RW CAREWare*:

1. Cuando las PVVS reciben servicios en las Organizaciones Sub Recipientes del Programa *Ryan White* Parte A y cuentan con el equipo y el sistema para la entrada de datos en tiempo real.
2. Cuando el usuario de la agencia donde reciben servicios las PVVS no está conectado en tiempo real a la base de datos del AME de San Juan.

El Programa *Ryan White* tiene establecida la Política y Procedimiento para la Asignación de Privilegios en el *RW CAREWare*.

V. Política y Procedimiento para la asignación de Privilegios en el RW CAREWare

Para garantizar la confidencialidad y privacidad de los datos en el Sistema *RW CAREWare*, se crearon estos procedimientos acorde con las políticas de seguridad electrónica del AME de San Juan. La información contenida y almacenada en el *RW CAREWare* no está disponible a todo usuario de la red del AME de San Juan o del propio sistema *RW CAREWare*. Dentro de *RW CAREWare* existe una jerarquía según el personal y el uso que se haga del sistema. La disponibilidad de información sobre pacientes o funciones propias del sistema *RW CAREWare* se asigna según el nivel de seguridad que se le adjudica al usuario. Ese nivel de seguridad depende del uso que el usuario tendrá del sistema.

A. Procedimiento I

Título:	Asignación de nivel de seguridad de Usuario del Sistema <i>RW CAREWare</i>
Fecha de Efectividad:	1 de enero de 2019
Revisado:	octubre 2018
Propósito:	Promover la seguridad, integridad y confidencialidad de los datos almacenados en el sistema <i>RW CAREWare</i> , todos los usuarios del <i>RW CAREWare</i> serán asignados a uno de los tres grupos que existen en el sistema

Procedimiento

Cada usuario debe ser entrevistado por el coordinador del sistema *RW CAREWare* y este determinará, según la función y la labor que realizará el usuario, a qué grupo pertenecerá.

El coordinador del *RW CAREWare* asignará los usuarios a tres grupos principales:

- *Data entry level* – usuarios que solamente entrarán datos al sistema
- *Power user* – usuarios que entrarán información al sistema pero que tienen la capacidad limitada para realizar transacciones administrativas, como por ejemplo: asignar contraseña (*password*) o crear informes de servicios
- Los administradores - usuarios que tienen privilegios para crear y ejecutar reportes, pero no entrar datos

No se puede asignar una contraseña (*password*) en *RW CAREWare* sin que el usuario haya sido clasificado en uno de estos tres grupos.

B. Procedimiento II

Título: Registro de usuario en *RW CAREWare*

Fecha de efectividad: 1 de enero de 2019

Revisado: octubre del 2018

Propósito: Promover la seguridad, integridad y confidencialidad de los datos almacenados en el sistema *RW CAREWare*. Todos los usuarios del *RW CAREWare* deberán ser orientados sobre la Ley *HIPAA* y tener firmado el Acuerdo de Confidencialidad y No Divulgación.

Procedimiento

Cada usuario del *RW CAREWare* deberá tener firmado el Acuerdo de Confidencialidad y No Divulgación, antes de que se le asigne un nombre de usuario (*username*) y una contraseña (*password*) en el sistema del *RW CAREWare*.

Este Acuerdo de Confidencialidad y No Divulgación se archivará en el expediente del empleado. Además, el empleado deberá mostrar competencia en los temas relacionados con la confidencialidad y la privacidad.

C. Procedimiento III

Título: Asignación de Usuario y Contraseña (*password*) en *RW CAREWare*

Fecha de efectividad: 1 de enero de 2019

Revisado: octubre de 2018

Propósito: Promover la seguridad, integridad y confidencialidad de los datos almacenados en el sistema del *RW CAREWare*. El coordinador del *RW CAREWare* será responsable de asignar nombres de usuarios (*usernames*) y contraseñas (*passwords*) a los usuarios, luego de que se cumplan con los procedimientos I y II de este documento

Procedimiento

Cada usuario del sistema deberá tener un nombre de usuario (*username*) y una contraseña (*password*) asignados por el coordinador del sistema del *RW CAREWare*.

El coordinador del *RW CAREWare* debe cumplir con la reglamentación y la política de uso apropiado de estaciones de trabajo (computadoras) del Departamento de Salud de Puerto Rico.

Los usuarios son los responsables de entrar la información que se documenta en las Hojas de Encuentro y en los expedientes médicos

VI. Política y Procedimiento para resguardo de la información del RW CAREWARE

El AME de San Juan reconoce que ningún proceso de resguardo es totalmente infalible o libre de la posibilidad de pérdida de información. La director(a) del Programa, junto con el personal del *RW CAREWare* y mediante procesos de análisis de riesgos, evaluarán las alternativas de resguardo para seguir identificando alternativas para proteger los activos de información del Programa.

El Programa creará copias fieles, exactas y recuperables del *e-PHI* bajo su custodia, cuando dicho *e-PHI* sea necesario para conducir el curso normal de trabajo del Programa.

Se requerirá que todo equipo computadorizado o electrónico que reciba, manipule, almacene o transmita *e- PHI*, sea sometido a un resguardo previo a cualquier movimiento del equipo.

Los resguardos (*back up*), deberán ser probados periódicamente, para asegurar que se están efectuando correctamente y que la información/datos en estos se pueda recobrar sin mayor dificultad.

Los resguardos (*back up*), se podrán almacenar en medios electrónicos que cumplan con los requerimientos de seguridad y encriptación de los datos.

Los medios de resguardo (*back up*) se deben rotar o alternar, para evitar dependencia en un medio particular que pueda sufrir desperfectos y exponga al Programa a no poder restaurar la información/datos de sus medios de resguardo.

Los programas originales y los resguardos (*back up*) de las bases de datos se guardan en un lugar contra incendio y los cuales permanecerán cerrados. La Directora(a) del Programa y el Gerente del *RW CAREWare* serán las únicas personas que tendrán acceso a estos archivos.

A. Procedimiento I

Título:	Movimiento de Equipo relacionado al e-PHI
Fecha de Efectividad:	1 de enero de 2019
Revisado:	octubre 2018
Propósito:	Promover la seguridad, integridad y confidencialidad de los datos almacenados y manipulados en computadoras que manipulen, reciban o transmita e-PHI.

Procedimiento

Identificar cada computadora, mediante inventario, de usuarios que puedan manipular recibir, almacenar o transmitir e-PHI.

El coordinador del *RW CAREWare* identificará cada equipo.

- Identificar el IP de la computadora (si aplica)
- Localizar donde se encuentra físicamente el equipo.
- Identificar quien es el usuario asignado a ese equipo.

B. Procedimiento II

Título: Frecuencia de los resguardos (Back up) de RW CAREWare

Fecha de Efectividad: 1 de enero de 2019

Revisado: octubre 2018

Propósito: La frecuencia de los resguardos (*back up*), como mínimo, deberá cumplir con las prácticas aceptables para datos críticos o la frecuencia adoptada como norma operacional por el sector de la salud para *e-PHI*. Sin embargo, el Programa hará todo lo posible para que la frecuencia de los resguardos (*back up*) sea de al menos un resguardo (*back up*) cada 24 horas.

Procedimiento

Se programará en el sistema RW CAREWARE que se produzca un resguardo de la data (BACK UP) cada 24 horas. El coordinador de RW CAREWare programará en el sistema la creación de dicho back up. Esto no invalida ningún otro procedimiento de resguardo adicional necesario y que se realizará fuera del sistema RW CAREWare

El coordinador del *RW CAREWare* identificara cada archivo de resguardo (back up) y se realizará lo siguiente:

- Identificar el back up
- Trasladar el archivo de resguardo a un servidor seguro donde se realizarán pruebas a la data recuperada.
- Este proceso se realizará una vez al mes, específicamente el último viernes de cada mes.

IV. Procedimiento para el manejo de quejas y/o querellas de las PVVS relacionadas a la privacidad y confidencialidad de los datos en RW CAREWARE

Propósito

Para garantizar la confidencialidad y privacidad de las quejas y/o querellas de las PVVS, se desarrolló este procedimiento acorde con las políticas de privacidad y confidencialidad y con las políticas de seguridad electrónica del AME de San Juan.

Procedimiento

Querellas de pacientes enviadas por correo o a través del personal del AME de San Juan o agencias y/u organizaciones contratadas:

- Las PVVS escriben sus quejas y/o querellas y las hacen llegar al personal del AME de San Juan.
- El personal del *RW CAREWare* responsable preparará informes trimestrales de quejas, para determinar el tipo y frecuencia de las quejas y el estatus de la solución de cada una. De ser necesario, se realizarán referidos adicionales o se presentarán recomendaciones para la resolución de las quejas activas

Estos informes se procederán a archivar en un archivo con llave ubicado en la oficina designada dentro del AME de San Juan.

Querellas de pacientes a través de correo electrónico:

- Las PVVS envían sus quejas y/o querellas a través del correo electrónico directamente al AME de San Juan a la dirección: emaatfsj@sanjuanciudadpatria.com con copia a emaatfsj@gmail.com o a través de los teléfonos del Programa
- Una vez se recibe la queja se le presenta al comité asesor de RW CAREWare quien a su vez informa a la directora(a) del Programa *Ryan White* Parte A y refiere la queja a la Unidad a la cual corresponda resolver el asunto. Una vez resuelto, comité asesor de CAREWare le informa al paciente del resultado de la queja, si el paciente ha ofrecido su información de contacto y se prepara un informe de cierre a la director(a) del Programa
- Los expedientes de las quejas son organizados en orden cronológico e identificados por el nombre de la organización contra la que se presenta la queja y la fecha

Estos expedientes serán ubicados en el archivo correspondiente bajo llave.